Kapitel 7

Schützen von Windows 10-Geräten

Wir wollen keine Panik schüren, aber jemand *ist* hinter Ihnen her. Computerangriffe nehmen von Jahr zu Jahr an Zahl und Schwere zu. Zwar finden die großen Datenverluste – Millionen von Kreditkartennummern bei einer großen Handelskette oder Millionen von Personalakten bei der US-Regierung – das größte Echo in den Medien, aber Sie brauchen sich nicht einzubilden, dass die Gauner nicht genauso gern in Ihren Computer eindringen würden. Ob es darum geht, Ihre wertvollen persönlichen Daten zu kopieren oder in Geiselhaft zu nehmen, Ihre Computerressourcen und Bandbreite abzuzweigen oder Ihren PC als Trittbrett beim Angriff auf ein größeres Ziel zu nutzen, mit dem Sie zu tun haben: Es gibt jede Menge Akteure, die Übles im Schilde führen.

Laut dem letzten Internet Security Threat Report von Symantec trafen im Jahr 2015 ganze 43 Prozent aller gezielten Angriffe Kleinunternehmen. Wie Privatpersonen haben solche Organisationen oft keine Mittel, die sie in die Sicherheit investieren könnten. Das macht sie zu verlockenden Zielen. Angestellte großer Organisationen werden eher über sogenanntes »Spear Phishing« angegriffen (sorgfältig auf die Zielperson zugeschnittenes Phishing), wenn ein Krimineller von außerhalb in andernfalls sichere Netzwerke einzudringen versucht.

In diesem Kapitel untersuchen wir, welcher Art von Bedrohungen Sie zu Hause und bei der Arbeit am ehesten ausgesetzt sind. Vor allem beschreiben wir einige der deutlichen Sicherheitsverbesserungen, die in Microsoft Windows 10 vorgenommen wurden. Viele davon betreffen Schichten, die Sie nicht sehen können, zum Beispiel der hardwarebasierte Schutz, der zum Einsatz kommt, noch bevor Windows geladen wird. Anschließend erklären wir die Benutzung der Sicherheitsfeatures, die Sie direkt sehen, darunter Windows-Firewall, Benutzerkontensteuerung, BitLocker und Windows Defender.

Sicherheitsbedrohungen

Vor etwa zehn Jahren waren die maßgebliche Bedrohung für Windows-Benutzer Viren und Würmer. Ach ja, die idyllischen alten Zeiten! Die moderne Bedrohungssituation ist viel komplexer und leider auch heimtückischer. Heutzutage ist ein Angreifer wahrscheinlich Mitglied einer organisierten Verbrecherbande oder sogar Mitarbeiter einer staatlichen Behörde, kein halbstarker Wichtigtuer, und die Angriffe sind meist mit dem Ziel geplant, dass sie möglichst lange unbemerkt bleiben.

Ein böswilliges Programm, das ohne Ihr Wissen installiert wurde und läuft, ohne dass Sie etwas davon ahnen, kann Schaden anrichten und Daten ohne Ihre Zustimmung übertragen. Diese Art von Software wird oft als *Schadsoftware* oder *Malware* bezeichnet.

Das Ziel der Angreifer besteht darin, Sie dazu zu bringen, ihre Software auszuführen. Zum Beispiel versucht jemand, Sie davon zu überzeugen, einen *Trojaner* (genauer ein trojanisches Pferd) zu installieren, das heißt ein Programm, das seriös aussieht, aber in Wirklichkeit böswillige Aktionen ausführt, sobald es installiert wurde. Diese Kategorie von Schadsoftware verbreitet sich nicht von allein, sondern versucht die Opfer mithilfe von »Social Engineering« (oft über beliebte soziale Netzwerke wie Facebook und Twitter) dazu zu bringen, beim Installationsvorgang zu helfen. In seinen Nutzdaten verborgen kann ein Trojaner einen Downloader umfassen, der weitere böswillige und unerwünschte Programme installiert. Manche Trojaner installieren eine Backdoor (Hintertür), über die ein externer Angreifer den infizierten Computer im Remotezugriff kontrolliert.

Worauf haben es die Angreifer abgesehen? Vor allem auf Geld, das auf unterschiedliche Arten eingenommen wird. Die Details hängen davon ab, wie die Angreifer durch Ihre Abwehrmaßnahmen gelangen. Hier einige Beispiele:

- Ein *Kennwortlogger* oder »Password Stealer« läuft im Hintergrund, zeichnet Benutzernamen und Kennwörter auf und leitet sie an einen externen Angreifer weiter. Die gestohlenen Anmeldeinformationen werden dann benutzt, um Waren zu kaufen, Bankkonten zu plündern oder Identitätsdiebstahl zu begehen.
- Angreifer machen sich Angst zunutze, indem sie gefälschte Sicherheitssoftware (sogenannte *Scareware*, »Erschreck-Software«) vertreiben, die Aktionen und Optik seriöser Antiviren-Software imitiert. Falls Sie ein solches Programm installieren, meldet es das Vorhandensein eines (herbeifantasierten) Virus und bietet an, ihn zu entfernen – gegen eine großzügige Gebühr natürlich.
- Im Jahr 2016 ist der Spitzenreiter bei Schadsoftware die sogenannte *Ransomware* (»Lösegeld-Software«), eine Form digitaler Erpressung, bei der ein Programm all Ihre Datendateien verschlüsselt und anbietet, sie nur gegen Zahlung eines Lösegelds wieder zu entschlüsseln.
- *Phishing-Angriffe* versuchen mithilfe von Social Engineering, Besucher dazu zu bringen, ihre Anmeldeinformationen zu verraten. Dies ist eine spezielle und bisweilen verheerende Form des Identitätsdiebstahls, die in jedem Browser unter jedem Betriebssystem zuschlagen kann.

Listen aktueller Schadsoftwarebedrohungen mit Links zu den jeweiligen Details finden Sie im Microsoft Malware Protection Center unter *https://bit.ly/malware-encyclopedia*. Einen umfassenderen Bericht zu der sich ständig verändernden Gefahrensituation veröffentlicht das Microsoft Malware Protection Center zweimal jährlich. Er wertet Daten von Hunderten von Millionen von Windows-Benutzern und andere Quellen aus. Die neueste Version dieses Microsoft Security Intelligence Report finden Sie unter *https://microsoft.com/security/sir*.

Schützen Ihres Computers: Strategien für eine gestaffelte Verteidigung

Eine komplexe Gefahrenlage erfordert einen mehrstufigen Ansatz, um Ihren PC und Ihr Netzwerk zu schützen. Das Ziel besteht letztlich darin, Ihr Gerät, Ihre Daten und Ihre Identität zu schützen sowie Schadsoftware zu blockieren. In einem Heim- oder kleinen Unternehmensnetzwerk sind die wichtigsten Sicherheitsmaßnahmen:

- **Schützen Sie Ihre Breitbandverbindung mit einem Hardwarerouter.** Dies ist ein wichtiger Teil der physischen Sicherheit, sogar wenn Ihr Netzwerk lediglich aus einem einzigen PC besteht. Einen Überblick über diese Komponenten finden Sie im Abschnitt »Grundlagen von Windows 10-Netzwerken« in Kapitel 5, »Grundlagen von Netzwerken«.
- **Aktivieren Sie eine Softwarefirewall und lassen Sie sie eingeschaltet.** Sie können die Windows-Firewall verwenden, die in Windows 10 enthalten ist, oder eine Firewall, die Sie sich aus einer anderen Quelle besorgen, beispielsweise aus einem der verbreiteten Security Suite-Pakete. Mehr zu diesem Thema finden Sie im Abschnitt »Abbildung « weiter unten in diesem Kapitel.
- **Nutzen Sie biometrische Anmeldeverfahren.** Biometrische Anmeldeverfahren arbeiten mit einem Fingerabdruckleser oder Gesichtserkennung mit Windows Hello. Sie bieten wesentlich mehr als lediglich Bequemlichkeit. Weil die biometrische Anmeldung mit einem bestimmten Gerät verknüpft ist, erhalten Sie eine effektive Zwei-Komponenten-Authentifizierung. Wenn Ihnen die nötige Hardware fehlt, können Sie eine PIN oder einen Bildcode für die Anmeldung verwenden, beide können sicherer sein als ein herkömmliches Kennwort. Weitere Informationen finden Sie im Abschnitt »Verwalten des Anmeldevorgangs« in Kapitel 6, »Verwalten von Benutzerkonten, Kennwörtern und Anmeldeinformationen«.
- **Legen Sie Standardbenutzerkonten an und lassen Sie die Benutzerkontensteuerung aktiviert.** Standardkonten helfen dabei, den Schaden, den ein ahnungsloser Benutzer anrichtet, indem er nicht vertrauenswürdige Programme installiert, zu verhindern oder wenigstens zu minimieren. Die Benutzerkontensteuerung (User Account Control, UAC) hilft Ihnen dabei, weil sie den Zugriff auf administrative Aufgaben beschränkt und Änderungen an Registrierung und Dateisystem virtualisiert. Einzelheiten finden Sie im Abschnitt »Einführung in die Zugangssteuerung von Windows« in Kapitel 6 und in »Unsichere Aktionen mit der Benutzerkontensteuerung verhindern« weiter unten in diesem Kapitel.
- **Halten Sie Windows und verwundbare Programme auf dem neuesten Stand.** Windows Update erledigt diese Aufgabe für Windows, Office und andere Microsoft-Programme. Bei Programmen anderer Hersteller müssen Sie selbst aktiv werden. Einen Überblick über Sicherheitsupdates finden Sie im Abschnitt »Sicherheitsupdates auf dem neuesten Stand halten« weiter unten in diesem Kapitel.
- **Verwenden Sie ein Antischadsoftware-Programm und halten Sie es auf dem neuesten Stand.** Windows Defender, das in Windows 10 enthalten ist, bietet Schutz vor Schadsoftware, es werden aber auch viele Lösungen anderer Hersteller angeboten. Einzelheiten finden Sie im Abschnitt »Blockieren von Schadsoftware mit Windows Defender« weiter unten in diesem Kapitel.

- **Schützen Sie sich vor Bedrohungen in E-Mail-Nachrichten.** Ihre E-Mail-Lösung sollte zumindest ausführbare Dateien und andere potenziell gefährliche Anhänge blockieren oder in Quarantäne legen. Außerdem können effektive Anti-Spam-Funktionen Skripts blockieren und Phishing-Versuche verhindern.
- **Verwenden Sie Jugendschutzeinstellungen, um Minderjährige zu schützen.** Wenn Sie Kinder im Haushalt haben, die Ihren Computer benutzen, helfen Ihnen die Family-Safety-Features in Windows, sie vor Sicherheitsbedrohungen zu schützen und zu verhindern, dass sie ungeeignete Sites besuchen. Sie finden dort Einstellmöglichkeiten, mit denen Sie die Computeraktivitäten von Kindern auf unterschiedliche Arten einschränken können. Einzelheiten finden Sie im Abschnitt »Beschränken der Zeit am Computer« in Kapitel 6.

Die Systemsteuerungs-App *Sicherheit und Wartung* überwacht viele dieser Bereiche und stellt sicher, dass Sie geschützt bleiben. Sie zeigt eine Warnung an, falls etwas Ihrer Aufmerksamkeit bedarf. Einzelheiten finden Sie im Abschnitt »Überwachen der Sicherheit Ihres Computers« weiter unten in diesem Kapitel.

Die wichtigsten Schutzmaßnahmen, die aber leider oft vergessen werden, sind Schulung der Benutzer und Selbstbeherrschung. Jeder, der einen Computer einsetzt, muss die Disziplin besitzen, Sicherheitsmeldungen zu lesen und zu befolgen, wenn sie angezeigt werden. Sie dürfen die Installation von Software nur erlauben, wenn klar ist, dass sie sicher ist. (Ein Benutzer, der über ein Standardkonto verfügt, kann kein Programm installieren oder ausführen, das den gesamten Computer leer räumt. Er kann aber trotzdem sein eigenes Benutzerprofil so stark beschädigen, dass erhebliche Mühe für die Reparatur aufgewendet werden muss.) Unzählige erfolgreiche Schadsoftwareangriffe weltweit haben bewiesen, dass viele Benutzer die Ratschläge für sichere Computernutzung nicht befolgen.

Neue Sicherheitsfeatures in Windows 10

Weil die Angreifer ihre Methoden ständig weiterentwickeln, ist ein wichtiges Verkaufsargument bei jeder neuen Windows-Version der Fortschritt im Bereich neuer und verbesserter Sicherheitsfeatures. Windows 10 ist hier keine Ausnahme. In diesem Abschnitt stellen wir die Änderungen in Windows 10 Home und Windows 10 Pro vor, Windows 10 Enterprise bietet in einem verwalteten Netzwerk noch etliche weitere Features.

Schützen von Geräten

Die Sicherheitsfunktionen in Windows 10 beginnen bei der Unterstützung moderner Hardwaredesigns. Windows 10 unterstützt zwar weiterhin ältere Hardware, aber manche Sicherheitsfeatures erfordern zwei Elemente, die in den meisten neueren Computern eingebaut sind:

- **Unified Extensible Firmware Interface (UEFI)** UEFI ist eine Firmwareschnittstelle, die das BIOS ersetzt, wie es seit den ersten PCs in jedem Computer vorhanden war. Neben anderen Verbesserungen ermöglicht UEFI den sicheren Gerätestart (Secure Boot) und die Geräteverschlüsselung (Device Encryption). Diese Features werden weiter unten beschrieben. PCs, die für Windows 8 oder eine neuere Version entwickelt wurden, müssen UEFI nutzen.

- **Trusted Platform Module (TPM)** Ein TPM ist ein Hardwarechip, der Verschlüsselung unterstützt und das Ändern oder Exportieren von Verschlüsselungsschlüsseln und Zertifikaten verhindert. Mit einem TPM ist es einfacher, die BitLocker-Laufwerkverschlüsselung (weiter unten in diesem Kapitel beschrieben) zu aktivieren. Andere Sicherheitsfeatures in Windows 10, zum Beispiel kontrollierter Start (Measured Boot) und DeviceGuard, setzen ein TPM voraus.

Sind UEFI und TPM vorhanden, kann Windows 10 den Startprozess absichern. (Viele neuere Schadsoftware-Angriffe übernehmen in einer frühen Phase des Startprozesses die Kontrolle über das System, noch bevor Windows vollständig läuft und Antischadsoftware-Programme in Aktion treten. Diese Art von Schadsoftware wird als *Rootkit* bezeichnet.) Der Windows 10-Startprozess durchläuft folgende Schritte:

- **Sicherer Start (Secure Boot)** Der sichere Start, eine Basisfunktion von UEFI, verhindert, dass ein anderes Betriebssystem-Ladeprogramm zum Einsatz kommt. Nur ein Betriebssystem-Ladeprogramm, das mit einem im UEFI gespeicherten Zertifikat digital signiert wurde, darf starten. (Ein herkömmliches BIOS erlaubt die Unterbrechung des Startprozesses, um ein beliebiges Betriebssystem-Ladeprogramm auszuführen, sogar wenn es beschädigt oder von Schadsoftware befallen ist.)
- **Antischadsoftware-Frühstart (Early Launch Antimalware, ELAM)** Antischadsoftware-Programme, die von Microsoft zertifiziert und signiert wurden (darunter fallen neben Windows Defender auch kompatible Programme anderer Hersteller), laden ihre Treiber vor jeglichen anderen Treibern oder Programmen anderer Hersteller. Dank dieses Ablaufs ist das Antischadsoftware-Programm in der Lage, Versuche zum Laden von Schadcode zu erkennen und zu verhindern.
- **Kontrollierter Start (Measured Boot)** Während des Starts werden Analysen der UEFI-Firmware und aller Windows-Komponenten vorgenommen. Die Ergebnisse werden dann digital signiert und im TPM gespeichert, wo sie nicht geändert werden können. Während nachfolgender Systemstarts werden die neuen Analysen mit den gespeicherten Ergebnissen verglichen.

Schützen von Daten

Die Verbreitung tragbarer PCs hat auch die Gefahr von Diebstahl erhöht. Einen Computer zu verlieren, ist übel genug, aber weit schlimmer ist es, wenn auch noch alle Daten, die Sie auf dem Computer gespeichert haben, in die falschen Hände gelangen. Windows 10 bietet neue Features, um sicherzustellen, dass der Dieb nicht an Ihre Daten gelangt:

- **Geräteverschlüsselung** Auf Geräten, die InstantGo unterstützen, werden die Daten auf dem Betriebssystemvolume standardmäßig verschlüsselt. (Dieses Feature hieß früher Connected Standby. InstantGo ist eine Microsoft-Hardwarespezifikation, die erweiterte Energieverwaltungsfunktionen ermöglicht. Neben anderen Anforderungen müssen InstantGo-Geräte von einem Solid-State-Laufwerk starten.) Die Verschlüsselung verwendet anfangs einen leeren Schlüssel, aber sobald sich erstmals ein lokaler Administrator mit einem Microsoft-Konto anmeldet, wird das Volume automatisch verschlüsselt. Ein Wiederherstellungsschlüssel steht zur Verfügung, wenn Sie sich unter dem entsprechenden Microsoft-Konto auf *https://onedrive.com/recoverykey* anmelden; Sie brauchen diesen Schlüssel, falls Sie das Betriebssystem neu installieren oder das Laufwerk in einen neuen PC einbauen wollen.

- **BitLocker-Laufwerkverschlüsselung** BitLocker-Laufwerkverschlüsselung bietet ähnliche (aber stärkere) Verschlüsselung von gesamten Volumes, und in Unternehmensnetzwerken ermöglicht sie eine zentrale Verwaltung. In Windows 10 verschlüsselt BitLocker Laufwerke schneller als in älteren Windows-Versionen. Weitere Geschwindigkeitsvorteile bringt die neue Fähigkeit, lediglich einen Teil eines benutzten Volumes zu verschlüsseln. Weitere Informationen finden Sie im Abschnitt »Verschlüsseln mit BitLocker und BitLocker To Go« weiter unten in diesem Kapitel.

Schützen von Identitätsdaten

Es scheint keine Woche zu vergehen, in der nicht über neue Fälle berichtet wird, bei denen Millionen von Benutzernamen und Kennwörtern ausgespäht wurden. Es gibt einen boomenden Markt für diese Art von Daten, weil sich Diebe damit überall mithilfe Ihrer Daten anmelden können. Und weil viele Leute auch noch dasselbe Kennwort für unterschiedliche Konten verwenden, schaffen es Kriminelle oft, mithilfe der gestohlenen Daten in andere Konten der Opfer einzubrechen. Windows 10 leitet den Anfang vom Ende der Kennwörter ein.

In Windows 10 ist eine unternehmensgeeignete Zwei-Komponenten-Authentifizierung namens Windows Hello eingebaut. Sobald ein Gerät bei einem Authentifizierungsdienst registriert wurde, wird das Gerät selbst ein Authentifizierungsfaktor. Der zweite Faktor ist eine PIN oder ein biometrisches Merkmal, zum Beispiel ein Fingerabdruck, eine Gesichtserkennung oder ein Netzhautscan.

Nachdem Windows Hello Sie angemeldet hat, ermöglicht es die Anmeldung bei Netzwerken und Webdiensten. Windows Hello unterstützt Microsoft-Konten, Active Directory- und Azure Active Directory-Konten (Azure AD) sowie alle Identitätsanbieter, die den Standard Fast ID Online (FIDO) v2.0 unterstützen. Ihre biometrischen Daten bleiben sicher im TPM Ihres Computers gespeichert, sie werden nicht über das Netzwerk versendet. (In der Erstversion von Windows 10 wurde dieses Feature für sichere Anmeldung als Microsoft Passport bezeichnet. Seit dem Anniversary Update ist es eine Teilkomponente von Windows Hello.)

Mit dieser Kombination von Authentifizierungsmethoden wird ein Angreifer gestoppt, auch wenn er noch so viele Benutzernamen und Kennwörter ausgespäht hat. Um Ihre verschlüsselten Daten zu entsperren (und somit die Fähigkeit zu erlangen, sich bei Ihren Webdiensten anzumelden), braucht er das registrierte Gerät. Und ein Dieb, der Ihren Computer stiehlt, braucht Ihre PIN oder Ihre biometrischen Daten. Active Directory, Azure Active Directory und Microsoft-Konten unterstützen bereits diese neue Form von Anmeldeinformationen, andere Dienste werden sicherlich folgen.

▶ **Weitere Informationen über Windows Hello finden Sie im Abschnitt »Verwalten des Anmeldevorgangs« in Kapitel 6.**

Blockieren von Schadsoftware

Seit den Tagen von Windows 7 wurden verschiedene Features optimiert, die böswillige Software blockieren:

- **Zufällige Anordnung des Layouts des Adressraums (Address Space Layout Randomization, ASLR)** ASLR ist ein Feature, das die Position von Programmcode und anderen Daten im Arbeitsspeicher wahllos verschiebt. Dadurch wird es für Schadsoft-

ware schwieriger, Angriffe auszuführen, die direkt in Systemspeicher schreiben, weil sie die benötigte Speicherstelle nicht findet. In Windows 10 werden Arbeitsspeicheradressen sogar noch stärker verwürfelt. Und weil die Zufallsfaktoren auf jedem Gerät anders sind, funktioniert ein Angriff, der auf einem Gerät erfolgreich war, auf einem anderen nicht.

- **Datenausführungsverhinderung (Data Execution Prevention, DEP)** DEP ist eine Hardwarefunktion, die Blöcke des Arbeitsspeichers so markiert, dass sie nur Daten speichern, aber keine Programmanweisungen ausführen dürfen. Windows 10 kann nur auf einem System installiert werden, das DEP anbietet.
- **Windows Defender** In Windows 7 war Windows Defender ein schlankes Antispyware-Programm. Seit Windows 8 wurden die bewährten Antischadsoftware-Fähigkeiten von Windows Security Essentials, einem kostenlosen Add-On für Windows 7, in Windows Defender integriert. Windows Defender unterstützt ELAM, wie weiter oben in diesem Kapitel beschrieben. Das bedeutet, dass er Schutz vor Rootkits bietet, die versuchen, sich in den Startprozess einzuschmuggeln. Weitere Informationen finden Sie im Abschnitt »Blockieren von Schadsoftware mit Windows Defender« weiter unten in diesem Kapitel.
- **SmartScreen** Die Aufgabe von SmartScreen ähnelt dem von Windows Defender: verhindern, dass böswilliger Code ausgeführt wird. Das ist wesentlich besser, als später zu versuchen, den Schaden zu beseitigen, der durch einen erfolgreichen Angriff verursacht wurde. Aber SmartScreen verfolgt einen völlig anderen Ansatz: Statt nach Signaturen bekannter Schadsoftware zu suchen, sucht er den Hashwert jeder ausführbaren Datei, die von einer Onlinequelle heruntergeladen wurde, in Microsofts Datenbank für Anwendungsbewertung. Dateien, die eine positive Bewertung haben, werden als sicher eingestuft und dürfen laufen, während Dateien mit negativer Bewertung (oder solche, die unbekannt und potenziell gefährlich sind) blockiert werden.

  Als SmartScreen in Windows 7 eingeführt wurde, war es ein Feature des Internet Explorers. Seit Windows 8 ist SmartScreen direkt in Windows integriert (und ist weiterhin ein Feature von Internet Explorer und, in Windows 10, von Microsoft Edge). Daher blockiert es die Ausführung aller unbekannten Programme, die aus einer Onlinequelle stammen. Das betrifft nicht nur Programme, die in einem Browser heruntergeladen wurden; SmartScreen wird immer aktiv, wenn Sie versuchen, ein solches Programm auszuführen.

Überwachen der Sicherheit Ihres Computers

In Windows 10 stehen die sicherheitsrelevanten Optionen im Systemsteuerungsmodul *Sicherheit und Wartung* zur Verfügung (Abbildung 7.1), das Sie über *Systemsteuerung/System und Sicherheit* erreichen. Erfahrene Windows 7- und Windows 8-Benutzer sehen, dass es sich um einen neuen Namen für das Wartungscenter in diesen älteren Betriebssystemen handelt. Sie können *Sicherheit und Wartung* über die Systemsteuerung oder die Einstellungen-App öffnen: Geben Sie im Suchfeld jeweils **Sicherheit** ein und klicken Sie auf *Sicherheit und Wartung*.

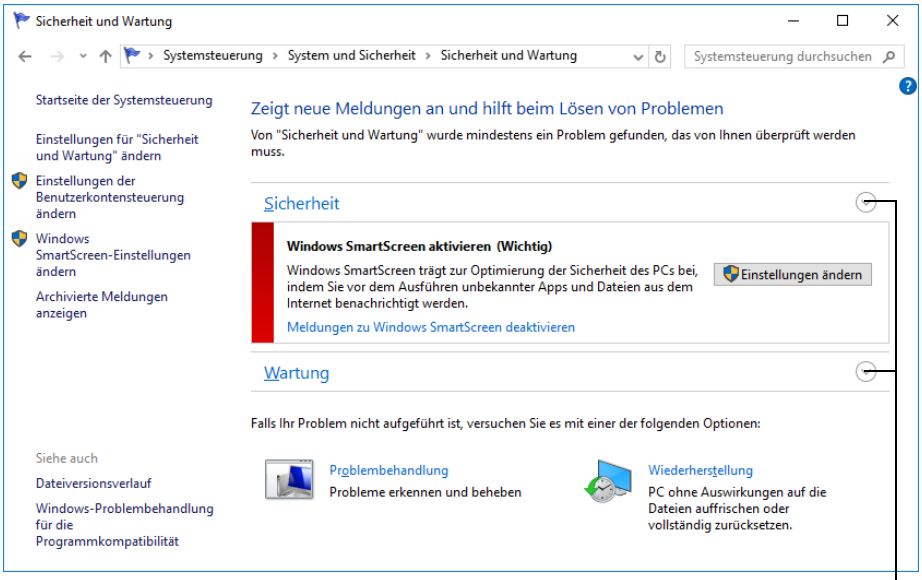

Abbildung 7.1 Das Modul *Sicherheit und Wartung* versammelt Sicherheits-, Wartungs- und Problembehandlungsinformationen sowie -einstellungen in einem einzigen Fenster. Potenzielle Probleme werden mit roten oder gelben Balken hervorgehoben.

Der Abschnitt *Sicherheit* im Fenster *Sicherheit und Wartung* fasst die wichtigsten Informationen über Ihre Sicherheitseinstellungen zusammen. Elemente, die Ihre Aufmerksamkeit benötigen, sind mit einem roten oder gelben Balken markiert. Ein roter Balken identifiziert wichtige Elemente, um die Sie sich sofort kümmern sollten, zum Beispiel ein erkannter Virus, das Vorhandensein von Spyware oder dass keine Firewall aktiviert ist. Ein gelber Balken markiert Informationsnachrichten über mangelhafte, aber nicht dringende Einstellungen oder Statusmeldungen. Neben den Balken werden Erklärungen sowie Schaltflächen eingeblendet, mit denen Sie das Problem beseitigen können (oder *Sicherheit und Wartung* so konfigurieren können, dass es keine Warnungen mehr anzeigt).

Sofern alles in Ordnung ist, ist die Kategorie *Sicherheit* eingeklappt und Sie sehen keine Details zu dieser Kategorie, wenn Sie *Sicherheit und Wartung* öffnen. Wenn Sie auf das Pfeilsymbol klicken, um die Kategorie aufzuklappen, sehen Sie alle sicherheitsrelevanten Elemente, die *Sicherheit und Wartung* überwacht.

Sicherheit und Wartung ist so entworfen, dass es mit Firewalls, Antiviren-Software und Antispyware-Programmen anderer Hersteller ebenso zusammenarbeitet wie mit den in Windows eingebauten Programmen (Windows-Firewall und Windows Defender). Systeme, auf denen in irgendeiner dieser Kategorien mehrere Programme installiert sind, zeigen eine Liste der verfügbaren Optionen an. Wenn Sie auf den Link zum Anzeigen der installierten Programme klicken, öffnet sich ein Dialogfeld, in dem Sie alle installierten Programme einschalten können, die momentan deaktiviert sind (Abbildung 7.2).

Falls Sie in *Sicherheit und Wartung* nicht mit Warnungen über bestimmte Sicherheitsfeatures belästigt werden wollen, können Sie auf der Seite *Einstellungen für "Sicherheit und Wartung" ändern* anklicken. Nachdem Sie im entsprechenden Dialogfeld die Kontrollkästchen

der Elemente, die Sie nicht überwachen wollen, deaktiviert haben (Abbildung 7.3), erhalten Sie keine weiteren Warnungen. *Sicherheit und Wartung* zeigt den Status lediglich als *Derzeit nicht überwacht* an.

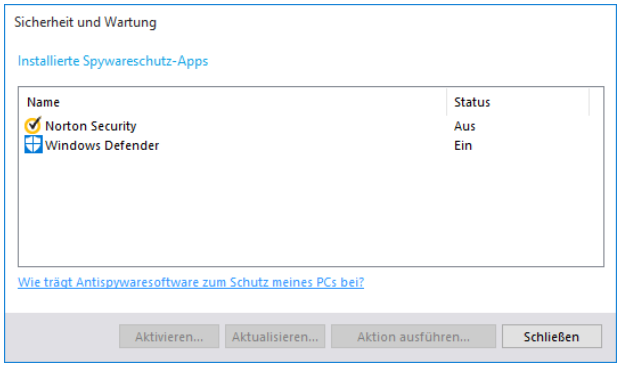

Abbildung 7.2 Wenn mehrere Schutzprogramme installiert sind, können Sie auf einen Link klicken, um eine solche Liste anzuzeigen

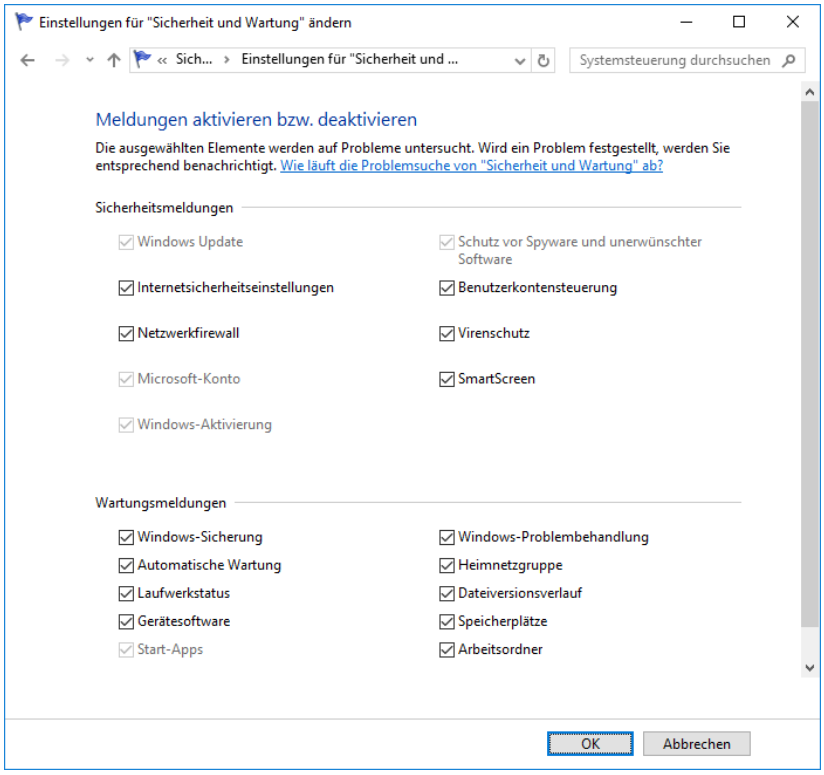

Abbildung 7.3 Auf dieser Seite können Sie die Überwachung ausgewählter Elemente in *Sicherheit und Wartung* individuell deaktivieren und aktivieren. Außerdem können Sie überwachte Elemente einzeln verwalten, indem Sie auf die Links im Fenster *Sicherheit und Wartung* klicken.

Sicherheitsupdates auf dem neuesten Stand halten

Wie bereits weiter oben in diesem Kapitel angemerkt, verbessert Microsoft die Sicherheit in Windows ständig weiter. Aber diese Aufgabe ist niemals abgeschlossen, weil sich ständig neue Bedrohungen entwickeln. Daher besteht die wahrscheinlich wichtigste Maßnahme, um Ihr System sicher zu halten, darin, dass Sie bei Updates für Windows und andere Programme stets auf dem neuesten Stand bleiben. Microsoft veröffentlicht häufig Updates, die installierte Gerätetreiber ersetzen und Code korrigieren, in dem Fehler entdeckt wurden. Manche Updates stellen neue Features zur Verfügung oder verbessern die Leistung, andere beheben Sicherheitslücken.

Um Updates automatisch zu installieren, greift Windows auf Windows Update zurück. Sie konfigurieren dieses Feature in der Einstellungen-App unter *Update und Sicherheit/Windows Update*. Weitere Informationen über Windows Update enthält der Abschnitt »Windows auf dem neuesten Stand halten« in Kapitel 15, »Systemwartung und -leistung«.

Vielleicht möchten Sie mehr über aktuelle Sicherheitsbedrohungen erfahren, besonders die, die von Windows Update behoben werden: Worin besteht die Bedrohung genau? Wie ernst ist sie? Wie lässt sie sich umgehen? Das Microsoft Security Response Center veröffentlicht detaillierte Informationen über eine Bedrohung und die Reaktion darauf in Form eines *Sicherheitsbulletins*.

Zu jedem kumulativen Update gibt es einen eigenen Knowledge Base-Artikel (KB), der anhand einer siebenstelligen Nummer identifiziert wird. Die Knowledge Base-Nummer für ein installiertes Update erfahren Sie, indem Sie auf *Updateverlauf* klicken. Wenn Sie nun auf den Installationslink unter einem Eintrag klicken, öffnet sich eine kurze Beschreibung dazu (Abbildung 7.4). Klicken Sie hier auf *Weitere Informationen*, um zum zugehörigen KB-Artikel zu gelangen.

Abbildung 7.4 Der Updateverlauf enthält Links, die zu weiteren Informationen über die einzelnen Updates führen

Dieser KB-Artikel enthält oft eine Liste der Sicherheitsupdates und anderen Fixes, die im kumulativen Update zusammengefasst sind, wobei es zu jedem einen eigenen KB-Artikel mit weiterführenden Informationen gibt. Sie können jeden KB-Artikel direkt lesen, indem Sie die URL *https://support.microsoft.com/kb/<nnnnnnn>/* aufrufen, wobei Sie <nnnnnnn> durch die siebenstellige Zahl ersetzen, die auf das Kürzel »KB« folgt.

Eine Liste der Sicherheitsbulletins liefert die Seite *Sicherheitshinweise und Bulletins* unter *https://bit.ly/security-advisories*. Hier finden Sie Links auf chronologisch sortierte Informationen (die neuesten zuerst) in folgenden Formaten:

- **Security Bulletin Summaries (Kurzzusammenfassung der Sicherheitsbulletins)** Jeden Monat wird ein Dokument mit einer vollständigen Liste aller Sicherheitsbulletins veröffentlicht, die im letzten Monat erschienen sind. In der Liste finden Sie zu jedem Bulletin den Titel und eine kurze Zusammenfassung, den Schweregrad (weiter unten in diesem Abschnitt werden diese Einstufungen genauer erklärt), eine Liste der betroffenen Software und einen Link auf das Bulletin.

  Sie gelangen direkt zur Zusammenfassung der monatlichen Sicherheitsbulletins, indem Sie die URL *https://technet.microsoft.com/library/security/ms<jj>-<mmm>/* verwenden, wobei Sie <jj> durch die beiden letzten Ziffern der Jahreszahl (zum Beispiel 16 für 2016) und <mmm> durch die englischsprachige Drei-Buchstaben-Abkürzung für den Monat (zum Beispiel »nov« für November) ersetzen.

- **Security Bulletins (Sicherheitsbulletins)** Jedes Bulletin enthält detaillierte Informationen über das Problem, darunter eine vollständige Liste der betroffenen Software (mit Versionsnummern) und eine Bewertung des Schweregrads, die bei Bedarf nach Versionsnummern aufgeschlüsselt ist. Jedes Sicherheitsbulletin bekommt einen Namen im folgenden Format zugewiesen: MS<jj>-<nnn>, wobei <jj> die letzten beiden Ziffern der Jahreszahl und <nnn> eine fortlaufende Nummer sind, die jedes Jahr mit 001 beginnt. Zum Beispiel trägt das siebenundzwanzigste Sicherheitsbulletin aus dem Jahr 2016 den Namen MS16-027.

  Sie können ein Sicherheitsbulletin direkt aufrufen, indem Sie seine Nummer an die URL *https://technet.microsoft.com/library/security/* anhängen.

- **Security Advisories (Sicherheitsempfehlungen)** Empfehlungen beschreiben Sicherheitsprobleme, die oft kein Sicherheitsbulletin (und kein Sicherheitsupdate) erfordern, sich aber dennoch auf die Sicherheit Ihres Computers auswirken können.

Jedes Sicherheitsbulletin enthält eine Einstufung für den Schweregrad der Bedrohung. Es werden vier Werte verwendet, sie sind hier von der schwerwiegendsten bis zur unkritischsten Bedrohung aufgeführt:

- **Kritisch (Critical)** Eine kritische Verwundbarkeit kann dazu führen, dass Code ohne Benutzerinteraktion ausgeführt wird.
- **Hoch (Important)** Eine hohe Verwundbarkeit kann so ausgenutzt werden, dass die Vertraulichkeit oder Integrität Ihrer Daten gefährdet ist oder dass ein Denial-of-Service-Angriff damit durchgeführt werden kann.

- **Mittel (Moderate)** Eine mittlere Verwundbarkeit lässt sich normalerweise durch Standardeinstellungen und Authentifizierungsanforderungen vermeiden. Anders ausgedrückt: Sie müssten sich recht ungeschickt anstellen, damit eine solche Bedrohung Ihr System oder Ihre Daten beschädigen kann.
- **Niedrig (Low)** Eine Verwundbarkeit von niedrigem Schweregrad kann normalerweise nur Schaden verursachen, wenn der Benutzer umfangreiche Interaktionen vornimmt oder eine ungewöhnliche Konfiguration vorliegt.

Weitere Informationen über diese Einstufungen finden Sie auf der Seite »Bewertungssystem für Security Bulletins« unter *https://bit.ly/severity-ratings*.

Aussperren von Eindringlingen mit der Windows-Firewall

Wenn es darum geht, Ihren Computer zu schützen, besteht die erste Verteidigungslinie meist darin, ihn vor Angriffen abzuschirmen, die von außen stammen. Sobald Ihr Computer mit dem Internet verbunden ist, wird er zu einem weiteren Knoten innerhalb eines gewaltigen globalen Netzwerks. Eine Firewall bildet eine Sperre zwischen Ihrem Computer und dem Netzwerk, mit dem er verbunden ist. Sie verhindert, dass unerwünschter Verkehr eingelassen wird, während autorisierte Verbindungen ohne Behinderung durchgelassen werden.

Der Einsatz einer Firewall ist simpel und unverzichtbar, oft wird sie gar nicht wahrgenommen. Stellen Sie unbedingt sicher, dass alle Netzwerkverbindungen durch eine Firewall geschützt werden. Zu Ihrer Beruhigung könnte beitragen, dass Ihr tragbarer Computer durch eine Unternehmensfirewall geschützt wird, während Sie bei der Arbeit sind, und zu Hause durch eine Router-Firewall. Aber was ist mit öffentlichen Hotspots, die Sie nutzen, während Sie unterwegs sind?

Es ist sogar dann sinnvoll, eine Firewall auf Ihrem Computer auszuführen, wenn Sie hinter einem heimischen Router oder der Unternehmensfirewall arbeiten. Andere Leute in Ihrem Netzwerk sind vielleicht nicht so sorgfältig wie Sie, wenn es um den Schutz vor Viren geht. Wenn daher jemand einen tragbaren Computer, der mit einem Wurm infiziert ist, zu Ihnen mitbringt und ihn an das Netzwerk anschließt, sind Sie erledigt – sofern Ihre Netzwerkverbindung nicht mit einer eigenen Firewall geschützt ist.

Windows enthält eine bidirektionale Firewall, die statusbehaftete Inspektion und Paketfilterung bietet. Ihr naheliegender Name ist Windows-Firewall. Die Windows-Firewall ist in der Standardeinstellung für alle Verbindungen aktiviert und beginnt schon beim Systemstart damit, Ihren Computer zu schützen. Die Firewall führt standardmäßig die folgenden Aktionen aus:

- Sie blockiert jeglichen eingehenden Verkehr, mit Ausnahme von Verkehr, der als Antwort auf eine Anforderung eintrifft, die Ihr Computer gesendet hat, und von unangefordertem Verkehr, den Sie durch Erstellen einer Regel explizit erlaubt haben.
- Sie erlaubt jeglichen ausgehenden Verkehr, sofern er einer konfigurierten Regel entspricht.

Sie bemerken nichts davon, wenn ein Paket verworfen wird, aber Sie können solche Ereignisse bei Bedarf in einem Protokoll aufzeichnen lassen.

Verwenden der Windows-Firewall mit unterschiedlichen Netzwerktypen

Die Windows-Firewall verwaltet für jeden der drei Netzwerktypen ein eigenes Profil (das heißt eine vollständige Sammlung von Einstellungen, inklusive Regeln für verschiedene Programme, Dienste und Ports):

- **Domäne** Wird benutzt, wenn Ihr Computer mit einer Active Directory-Domäne verbunden ist. In dieser Umgebung werden die Firewalleinstellungen üblicherweise (aber nicht zwingend) von einem Netzwerkadministrator konfiguriert.
- **Privat** Dieses Profil wird benutzt, wenn Ihr Computer mit einem Heim- oder Arbeitsplatznetzwerk in einer Arbeitsgruppenkonfiguration verbunden ist.
- **Gast oder öffentlich** Wird benutzt, wenn Ihr Computer mit einem Netzwerk an einem öffentlichen Ort verbunden ist, zum Beispiel auf einem Flughafen oder in einem Restaurant. Es ist üblich (und wird empfohlen), weniger Programme zu erlauben und stärkere Einschränkungen zu definieren, wenn Sie ein öffentliches Netzwerk benutzen.

Wenn Sie gleichzeitig mit mehreren Netzwerken verbunden sind (weil Sie zum Beispiel eine WLAN-Verbindung zu Ihrem Heimnetzwerk haben, während Sie über eine VPN-Verbindung mit Ihrer Unternehmensdomäne verbunden sind), verwendet Windows für jede Verbindung das passende Profil. Dafür ist ein Feature verantwortlich, das den Namen MAFP (Multiple Active Firewall Profiles) trägt.

Einstellungen nehmen Sie in der Windows-Firewall für jedes Netzwerkprofil getrennt vor. Die Einstellungen in einem Profil gelten für alle Netzwerke des jeweiligen Typs, zu denen Sie eine Verbindung herstellen. (Wenn Sie beispielsweise einem Programm den Zugriff durch die Firewall erlauben, während Sie mit einem öffentlichen Netzwerk verbunden sind, wird diese Programmregel immer aktiviert, wenn Sie mit einem anderen öffentlichen Netzwerk verbunden sind. Sie wird aber nicht aktiviert, wenn Sie mit einem Domänen- oder privaten Netzwerk verbunden sind; dazu müssten Sie das Programm explizit auch in diesen Profilen zulassen.)

▶ **Weitere Informationen über Netzwerktypen finden Sie im Abschnitt »Einstellen von Netzwerkstandorten« in Kapitel 5.**

Verwalten der Windows-Firewall

Die Windows-Firewall ist eine Systemsteuerungsanwendung mit einer simplen Benutzeroberfläche, in der Sie den Firewallstatus überwachen und Routineaufgaben durchführen können, zum Beispiel ein Programm durch die Firewall zulassen oder alle eingehenden Verbindungen blockieren. Sie öffnen die Windows-Firewall, indem Sie im Suchfeld oder in der Systemsteuerung **firewall** eintippen. Klicken Sie auf *Windows-Firewall*, um das gleichnamige Fenster zu öffnen (Abbildung 7.5).

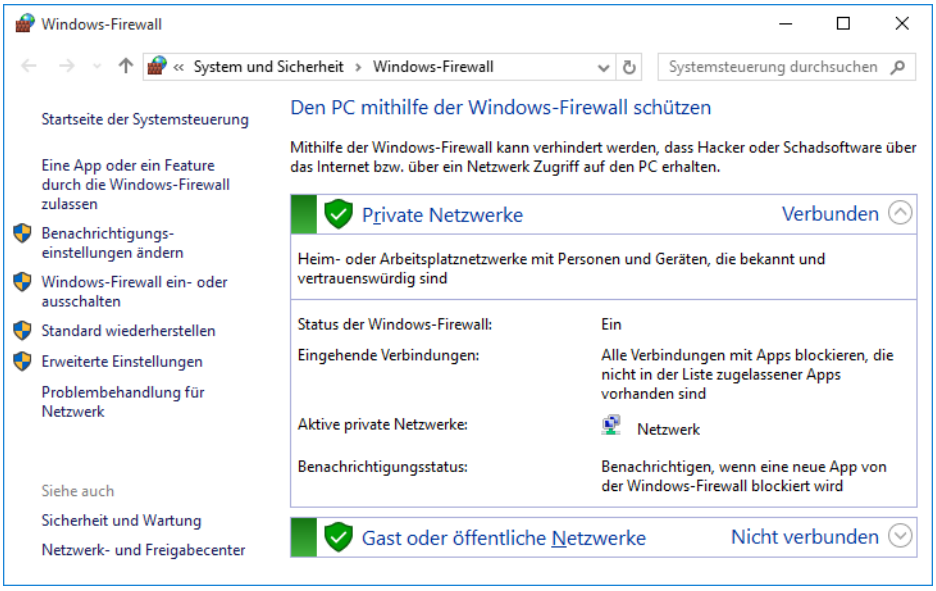

Abbildung 7.5 Die Windows-Firewall zeigt den Status und Einstellungen für jedes momentan verbundene Netzwerk an. Das Profil für Domänennetzwerke erscheint nur auf Computern, die einer Domäne beigetreten sind.

Aktivieren oder Deaktivieren der Windows-Firewall

Die in Abbildung 7.5 gezeigte Hauptanwendung der Windows-Firewall ist im Wesentlichen ein Statusfenster und ein Ausgangspunkt, um verschiedene Firewalleinstellungen vorzunehmen. Die erste interessante Einstellung bietet Ihnen die Möglichkeit, die Windows-Firewall zu aktivieren oder zu deaktivieren. Klicken Sie dazu auf *Windows-Firewall ein- oder ausschalten*. Daraufhin öffnet sich das Fenster aus Abbildung 7.6, in dem Sie die Windows-Firewall für jeden Netzwerktyp aktivieren (einschalten) oder deaktivieren (ausschalten) können. Im Allgemeinen gibt es nur zwei Gründe, die Windows-Firewall auszuschalten: im Rahmen der Problembehandlung, um kurz (und mit höchster Vorsicht) ein Verbindungsproblem zu analysieren, oder wenn Sie die Firewall eines anderen Herstellers installiert haben, die Sie statt der Windows-Firewall einsetzen möchten. Die meisten solcher Firewalls erledigen diesen Schritt allerdings automatisch im Rahmen des Installationsvorgangs.

Wie bereits erwähnt, sind Einstellungen für Domänennetzwerke in der Windows-Firewall nur verfügbar, wenn Sie tatsächlich einer Domäne beigetreten sind. Einstellungen für alle anderen Netzwerktypen können Sie jederzeit vornehmen, auch wenn Sie momentan nicht mit einem Netzwerk des entsprechenden Typs verbunden sind. Einstellungen für das Domänenprofil hat der Netzwerkadministrator allerdings oft mithilfe von Gruppenrichtlinien verriegelt.

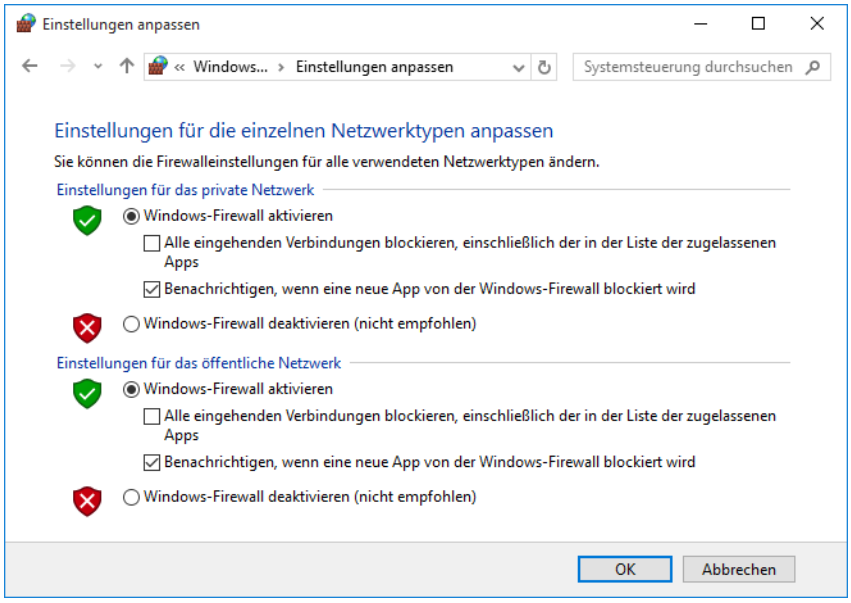

Abbildung 7.6 Aktivieren oder Deaktivieren der Windows-Firewall

Das Kontrollkästchen *Alle eingehenden Verbindungen blockieren* im Fenster *Einstellungen anpassen* bietet zusätzliche Sicherheit. Wenn es aktiviert ist, weist die Windows-Firewall jeglichen nicht-angeforderten eingehenden Verkehr ab, sogar wenn dieser Verkehr von erlaubten Programmen stammt oder eigentlich über eine Regel zugelassen wurde. (Informationen über Firewallregeln enthält der nächste Abschnitt, »Verbindungen durch die Firewall zulassen«.) Sie können diesen Modus einschalten, wenn Sie zusätzlichen Schutz vor externen Angriffen benötigen. Zum Beispiel können Sie alle Verbindungen blockieren, wenn Sie einen öffentlichen WLAN-Hotspot verwenden oder wissen, dass Ihr Computer momentan angegriffen wird.

Hinweis

Wenn Sie das Kontrollkästchen *Alle eingehenden Verbindungen blockieren* aktivieren, wird Ihr Computer nicht vom Internet abgeschnitten. Sogar in diesem Modus können Sie mit Ihrem Browser auf das Internet zugreifen. Auch andere ausgehende Verbindungen arbeiten ungehindert weiter – das gilt sowohl für berechtigte Dienste als auch für Spyware. Wenn Sie Ihre Verbindung zur Außenwelt wirklich kappen wollen, können Sie das Netzwerk- und Freigabecenter öffnen und alle Netzwerkverbindungen deaktivieren. (Stattdessen können Sie auch handgreiflich werden: Ziehen Sie Netzwerkkabel ab und schalten Sie WLAN-Adapter oder Zugriffspunkte aus.)

Verbindungen durch die Firewall zulassen

In manchen Situationen wollen Sie anderen Computern erlauben, eine Verbindung zu Ihrem Computer aufzubauen. Wenn Sie beispielsweise den Remotedesktop verwenden, sich mit Multiplayerspielen entspannen oder über ein Instant-Messaging-Programm chat-

ten, benötigen diese Programme üblicherweise eingehende Verbindungen, damit andere Leute zu Ihnen Kontakt aufnehmen können.

Am einfachsten können Sie für ein Programm, das keine eigenen Firewallregeln erstellt, eine Verbindung aktivieren, indem Sie auf *Eine App oder ein Feature durch die Windows-Firewall zulassen* klicken, einen Link auf der linken Seite des Hauptfensters *Windows-Firewall*. Welche Programme und Features anfangs im Fenster *Zugelassene Apps* aufgelistet werden (Abbildung 7.7), hängt davon ab, welche Programme und Dienste auf Ihrem Computer installiert sind. Sie können weitere hinzufügen, wie in den folgenden Abschnitten beschrieben. Außerdem werden Programmregeln erstellt (aber nicht aktiviert), wenn ein Programm versucht, eine eingehende Verbindung einzurichten. Um Verbindungen für ein Programm oder einen Dienst zu erlauben, nachdem sie bereits definiert wurden, brauchen Sie lediglich das entsprechende Kontrollkästchen für jeden Netzwerktyp zu aktivieren, in dem Sie das Programm zulassen wollen. (Sie müssen auf *Einstellungen ändern* klicken, bevor Sie Änderungen vornehmen können.)

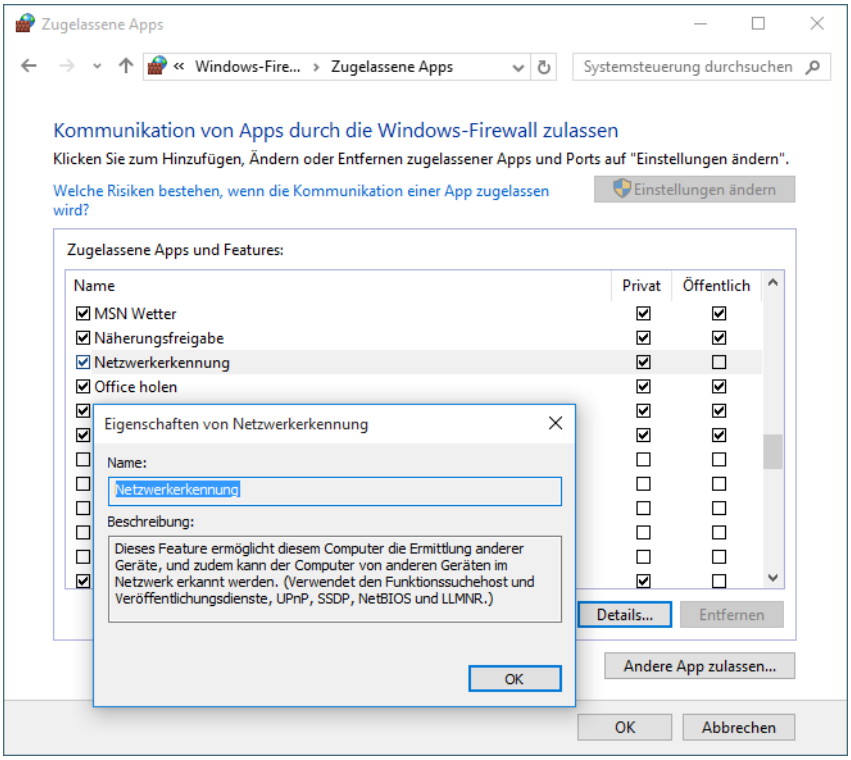

Abbildung 7.7 Wenn Sie einen Eintrag auswählen und auf *Details* klicken, wird eine Beschreibung des Programms oder Dienstes angezeigt

In all diesen Fällen aktivieren Sie in der Windows-Firewall eine Regel, die ein kleines Loch in die Firewall bohrt und erlaubt, dass eine bestimmte Art von Verkehr hindurchgelassen wird. Jede Regel dieses Typs verringert in einem gewissen Maß Ihre Sicherheit, daher sollten Sie die Kontrollkästchen aller Programme deaktivieren, die Sie nicht brauchen. Sofern Sie

sicher sind, dass Sie ein bestimmtes Programm niemals benötigen, können Sie es auch auswählen und auf *Entfernen* klicken. (Viele der Listenelemente, die in Windows für bestimmte Apps oder Dienste vordefiniert sind, lassen sich nicht löschen. Aber solange ihre Kontrollkästchen nicht aktiviert sind, bedeuten diese Apps keine Gefahr.)

Wenn Sie ein Programm, das versucht, eine eingehende Verbindung aufzubauen, zum ersten Mal starten, fragt die Windows-Firewall nach der entsprechenden Berechtigung, indem sie ein Dialogfeld anzeigt. Sie können das Programm zur Liste der erlaubten Programme hinzufügen, indem Sie auf *Zugriff zulassen* klicken.

Wenn ein solches Dialogfeld erscheint, sollten Sie es sorgfältig durchlesen und folgende Punkte durchdenken:

- Haben Sie das Programm, das eine Genehmigung fordert, wissentlich installiert und ausgeführt?
- Ist es vernünftig, dass für dieses Programm eingehende Verbindungen zugelassen werden?
- Verwenden Sie momentan einen Netzwerktyp, in dem es in Ordnung ist, wenn dieses Programm eingehende Verbindungen annimmt?

Falls die Antwort auf eine dieser Fragen Nein lautet oder falls Sie unsicher sind, sollten Sie auf *Abbrechen* klicken. Wenn Sie dann später feststellen, dass ein wichtiges Programm nicht einwandfrei funktioniert, können Sie in der Windows-Firewall die Liste der zugelassenen Apps öffnen und die Regel aktivieren.

Stattdessen können Sie die Ausnahme für das Programm auch im Fenster *Zugelassene Apps* einrichten (Abbildung 7.7), ohne darauf zu warten, dass sich eine Windows-Sicherheitswarnung öffnet. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf *Andere App zulassen*. Daraufhin öffnet sich das Dialogfeld *App hinzufügen*.
2. Wählen Sie in *App hinzufügen* das Programm aus, für das Sie eingehende Verbindungen erlauben wollen. Stattdessen können Sie auch auf *Durchsuchen* klicken und die ausführbare Datei auswählen, falls sie nicht in der Liste der Apps aufgeführt ist.
3. Klicken Sie auf *Netzwerktypen* (Abbildung 7.8).

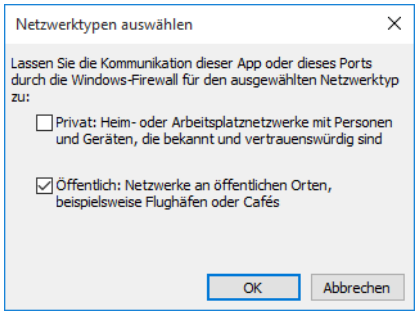

Abbildung 7.8 Zulassen von eingehenden Verbindungen für eine bestimmte App

4. Aktivieren Sie die Kontrollkästchen der Netzwerktypen, in denen Sie das Programm zulassen wollen, klicken Sie auf *OK* und dann auf *Hinzufügen*. (Sie können die Netzwerktypen auch im Fenster *Zugelassene Apps* auswählen, nachdem Sie das Programm hinzugefügt haben.)

Wiederherstellen der Standardeinstellungen

Falls Sie ein wenig mit der Windows-Firewall herumexperimentiert und Verbindungen erlaubt haben, die nicht sinnvoll sind, können Sie einen bekannt sicheren Zustand wiederherstellen, indem Sie im Fenster *Windows-Firewall* auf *Standard wiederherstellen* klicken. Dabei entfernen Sie allerdings alle Regeln, die Sie für diverse Programme hinzugefügt haben. Sie erhalten auf diese Weise zwar eine sichere Konfiguration, es kann aber passieren, dass einige netzwerkabhängige Programme nicht mehr richtig funktionieren. In einem solchen Fall können Sie die gewünschten Programme, die eine Genehmigung brauchen, wieder hinzufügen; dies wurde im letzten Abschnitt beschrieben.

Erweiterte Werkzeuge zum Verwalten der Windows-Firewall

Wenn Sie bereits Erfahrung mit dem Konfigurieren von Firewalls haben, wird Ihnen bald klar, dass die Systemsteuerungsanwendung *Windows-Firewall* lediglich die simpelsten Aufgaben abdeckt. Daraus dürfen Sie aber nicht ableiten, dass es der Windows-Firewall an Leistungsfähigkeit mangelt. Ganz im Gegenteil können Sie alle möglichen Firewallregeln konfigurieren und Verkehr abhängig von Programm, Port, Protokoll, IP-Adresse und anderen Faktoren erlauben oder blockieren. Außerdem können Sie Regeln aktivieren, deaktivieren und überwachen, eine Protokollierung konfigurieren und vieles weitere. Mit leistungsfähigen Werkzeugen können Sie auch die Windows-Firewall auf Remotecomputern konfigurieren. Weil die Benutzeroberfläche dieser erweiterten Features etwas einschüchternd wirkt, stellt die Windows-Firewall die vereinfachte Benutzeroberfläche zur Verfügung, die in den letzten Abschnitten beschrieben wurde. Sie eignet sich nicht nur für weniger erfahrene Benutzer, sondern auch für fortgeschrittene Benutzer und IT-Fachleute, die lediglich Routineaufgaben an der Firewall ausführen wollen.

Trotzdem wäre unser Überblick über die Sicherheitsfeatures nicht vollständig, würden wir die *Windows-Firewall mit erweiterter Sicherheit* übergehen, ein MMC-Snap-In (Microsoft Management Console), das Ihnen detaillierte Kontrolle über Regeln, Ausnahmen und Profile verschafft. Sie können es öffnen, indem Sie im Fenster *Windows-Firewall* auf *Erweiterte Einstellungen* klicken. Daraufhin öffnet sich die Konsole *Windows-Firewall mit erweiterter Sicherheit* (Abbildung 7.9).

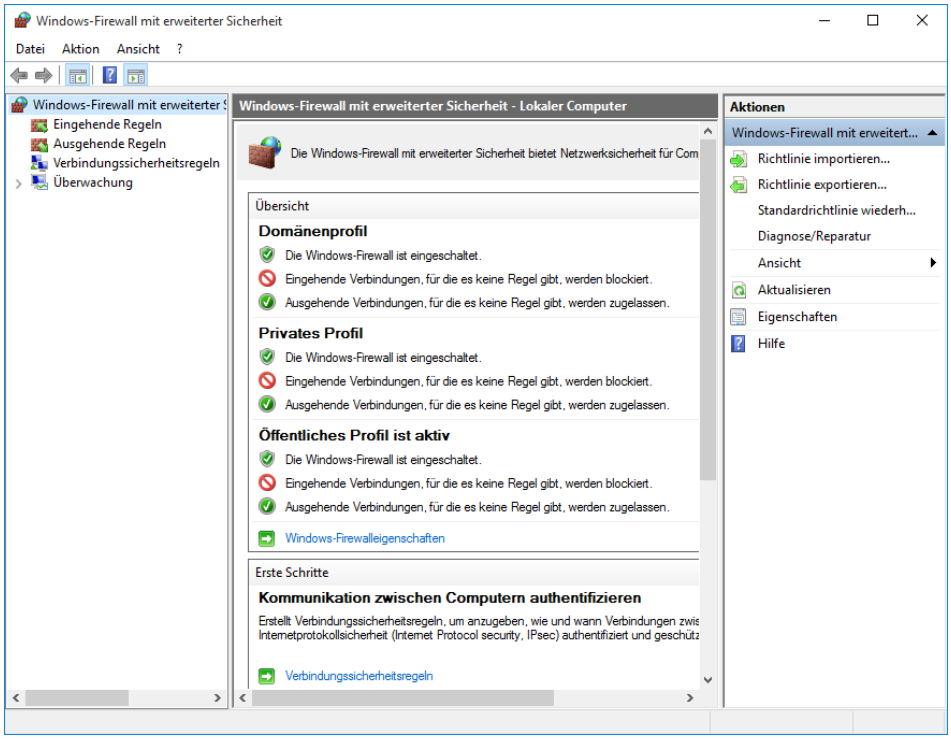

Abbildung 7.9 Klicken Sie im linken Fensterabschnitt auf *Eingehende Regeln* oder *Ausgehende Regeln*, um Firewallregeln anzusehen, zu konfigurieren, zu erstellen und zu löschen. Das Domänenprofil erscheint sogar auf einem Computer, der nicht Mitglied einer Windows-Domäne ist.

Die Konsole zeigt in der Standardeinstellung ähnliche Informationen an wie das Fenster *Windows-Firewall*. Sobald Sie sich allerdings einige Schritte in die Höhle hineinwagen, besteht die Gefahr, dass Sie sich verirren. Der Artikel »Windows-Firewall mit erweiterter Sicherheit« unter *https://aka.ms/firewall* ist ein brauchbarer Wegweiser.

Expertentipp

Windows-Firewall mit erweiterter Sicherheit direkt öffnen

Sie brauchen nicht die Systemsteuerungsanwendung *Windows-Firewall* zu öffnen, um zur Konsole *Windows-Firewall mit erweiterter Sicherheit* zu gelangen. Geben Sie im Suchfeld wf.msc und drücken Sie die Tastenkombination Strg + ⇧ + ↵, um die Konsole als Administrator auszuführen.

Unsichere Aktionen mit der Benutzerkontensteuerung verhindern

Die Benutzerkontensteuerung (User Account Control, UAC) zog sich vielfach regelrechten Hass zu, als sie vor zehn Jahren in Windows Vista eingeführt wurde. Sie greift immer ein, wenn ein Benutzer oder ein Programm versucht, eine administrative Aufgabe auszuführen, und fordert die Zustimmung eines Computeradministrators an, bevor sie die potenziell schädliche Operation beginnt. Seit den schwierigen Anfängen hat sich die UAC zu einer effektiven Sicherheitsmaßnahme entwickelt, auch weil sie nicht mehr so lästig ist wie die ursprüngliche Implementierung.

In Windows 10 sind Benutzerkonten, die Sie einrichten, zuerst einmal Standardkonten (keine Administratorkonten). Diese Konten können zwar die üblichen Arbeiten erledigen, sind aber nicht in der Lage, möglicherweise schädliche Operationen auszuführen. Diese Einschränkungen gelten nicht nur für den Benutzer, sondern vor allem für jegliche Programme, die von diesem Benutzer gestartet werden. Sogar Administratorkonten laufen als »geschützte« Administratorkonten, das heißt, dass sie normalerweise nur über Standardbenutzerprivilegien verfügen und nur dann höhere Privilegien erhalten, wenn sie tatsächlich administrative Aufgaben durchführen müssen. (Dies wird auch als Administratorbestätigungsmodus bezeichnet.)

▶ **Informationen über Benutzerkonten finden Sie in Kapitel 6.**

Die meisten Programme sind so geschrieben, dass sie keine Administratorprivilegien brauchen, um alltägliche Aufgaben zu erledigen. Programme, die tatsächlich administrativen Zugriff brauchen (zum Beispiel Dienstprogramme, die Computereinstellungen verändern), fordern eine Anhebung der Privilegien an. Und an dieser Stelle kommt die UAC ins Spiel.

Was löst UAC-Eingabeaufforderungen aus?

Zu den Aktionen, die eine Anhebung auf Administratorstatus brauchen (und folglich eine UAC-Anhebungseingabeaufforderung anzeigen), gehören alle, die Änderungen an systemweiten Einstellungen oder Dateien in *%SystemRoot%* oder *%ProgramFiles%* vornehmen. (Auf einer Windows-Standardinstallation stehen diese Umgebungsvariablen für die Ordner *C:\Windows* beziehungsweise *C:\Program Files*.) Unter anderem benötigen die folgenden Aktionen eine Privilegienanhebung:

- Installieren und Deinstallieren der meisten Desktopanwendungen
- Installieren von Gerätetreibern, die nicht in Windows enthalten sind oder über Windows Update ausgeliefert wurden
- Installieren von ActiveX-Steuerelementen
- Ändern von Einstellungen für die Windows-Firewall
- Ändern von UAC-Einstellungen
- Konfigurieren von Windows Update
- Hinzufügen oder Löschen von Benutzerkonten
- Ändern des Kontotyps für einen Benutzer

- Ausführen der Aufgabenplanung
- Bearbeiten der Registrierung
- Wiederherstellen gesicherter Systemdateien
- Anzeigen oder Ändern von Ordnern und Dateien eines anderen Benutzers

In Windows erkennen Sie viele Aktionen, die eine Privilegienanhebung benötigen, schon im Voraus. Ein Schildsymbol neben einer Schaltfläche oder einem Link zeigt an, dass sich eine UAC-Eingabeaufforderung öffnet, falls Sie ein Standardkonto verwenden (Abbildung 7.10).

Die Schildsymbole am linken Rand kennzeichnen Aktionen, die eine UAC-Anhebung erfordern

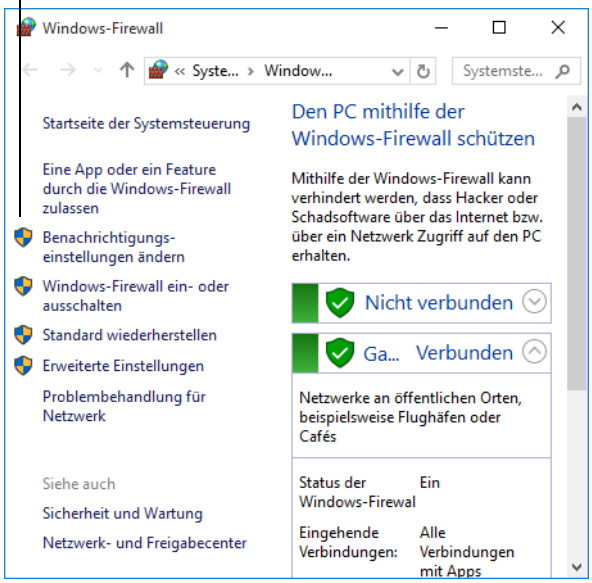

Abbildung 7.10 UAC-Symbole in der Systemsteuerung

Wenn Sie sich mit einem Administratorkonto anmelden (und die UAC-Standardeinstellungen unverändert lassen), erscheinen weniger Bestätigungsaufforderungen als unter einem Standardkonto. Das liegt daran, dass in der Standardeinstellung nur dann eine Bestätigung angefordert wird, wenn ein Programm versucht, Software zu installieren oder andere Änderungen am Computer vorzunehmen, aber nicht, wenn Sie selbst die Änderungen an Windows-Einstellungen durchführen – selbst wenn diese Änderungen bei einem Standardbenutzer mit UAC-Standardeinstellungen eine Eingabeaufforderung auslösen. Windows führt für bestimmte Programme, die Teil von Windows sind, eine automatische Privilegienanhebung ohne Eingabeanforderung durch. Programme, deren Privilegien automatisch auf diese Weise angehoben werden, stammen aus einer vordefinierten Liste, sie müssen vom Windows-Hersteller digital signiert und in bestimmten geschützten Ordnern gespeichert sein.

Die Grenzen der Benutzerkontensteuerung

Die Benutzerkontensteuerung ist kein Allheilmittel für alle Sicherheitsprobleme. Sie ist lediglich eine Schicht innerhalb einer mehrstufigen Verteidigungsstrategie.

Manche Windows-Benutzer nehmen an, dass die UAC-Bestätigungsaufforderungen eine Sicherheitshürde bilden. Das ist nicht der Fall. Sie sind lediglich eine Stelle, an der ein Administrator die Entscheidung trifft, ob er jemandem vertraut. Falls ein Angreifer es schafft, Sie über Social Engineering davon zu überzeugen, dass Sie unbedingt sein Programm brauchen, haben Sie bereits eine Vertrauensentscheidung getroffen. Sie machen mindestens ein halbes Dutzend Klicks, um sein hinterhältiges Programm herunterzuladen, zu speichern und zu starten. Eine UAC-Bestätigungsaufforderung fügt sich völlig natürlich in diese Ereigniskette ein, warum sollten Sie also nicht einen weiteren Mausklick machen?

Wenn Sie dieses Szenario beunruhigt, besteht die offensichtliche Lösung darin, die UAC mit ihren schärfsten Einstellungen zu konfigurieren. Neben anderen Änderungen deaktiviert diese Einstellung die automatische Privilegienanhebung. (Einzelheiten dazu finden Sie im Abschnitt »Ändern der UAC-Einstellungen« weiter unten in diesem Kapitel.) Falls ein Programm versucht, mithilfe dieser Täuschung Systemänderungen an Ihnen vorbei zu schmuggeln, bekommen Sie eine unerwartete Bestätigungsaufforderung vom System. Aber sobald Sie die erhöhten Anmeldeinformationen eingeben, kann der Code alles tun, was er will.

Ein besserer Ansatz ist es, sich mit einem Standardkonto anzumelden, das eine echte Sicherheitshürde aufbaut. Ein Standardbenutzer, der nicht über das Administratorkennwort verfügt, kann nur Änderungen an seinem eigenen Benutzerprofil vornehmen. Das System bleibt vor unbeabsichtigter Manipulation geschützt.

Aber sogar wenn Sie als Standardbenutzer arbeiten, bietet das keinen vollständigen Schutz. Schadsoftware kann in Ihrem Benutzerprofil installiert werden, ohne dass irgendwelche Systemalarme ausgelöst werden. Sie kann Ihre Tastatureingaben aufzeichnen, Ihre Kennwörter ausspähen, Ihre Datendateien verschlüsseln und Lösegeld für die Freigabe fordern oder E-Mail unter Ihrer Identität versenden. Selbst wenn Sie die UAC auf die höchste Sicherheitsstufe setzen, kann es passieren, dass Sie auf Schadsoftware hereinfallen, die nur darauf wartet, dass Sie Ihre Privilegien anheben. In diesem Moment schlägt sie zu und schmuggelt ihre Manipulationen unter dem Deckmantel Ihrer eigenen Operationen ein.

Um es noch einmal deutlich zu betonen: Das Aktivieren der UAC ist lediglich eine Maßnahme in einer mehrstufigen Sicherheitsstrategie. Sie funktioniert am besten, wenn sie durch gesundes Misstrauen und topaktuelle Antischadsoftware-Programme ergänzt wird.

UAC-Eingabeaufforderungen

Bei der Anmeldung generiert Windows ein Token, mit dem die Privilegstufen Ihres Kontos festgelegt werden. Standardbenutzer bekommen ein Standardtoken, aber Administratoren erhalten gleich zwei: ein Standardtoken und ein Administratortoken. Das Standardtoken wird benutzt, um *Explorer.exe* (die Windows-Shell) zu starten, aus der alle nachfolgenden Programme ausgeführt werden. Abgeleitete Prozesse erben das Token des Prozesses, der sie gestartet hat, daher laufen in der Standardeinstellung alle Anwendungen als Standardbenutzer – sogar wenn Sie sich mit einem Administratorkonto angemeldet haben. Bestimmte Programme fordern eine Anhebung auf Administratorprivilegien an, und an diesem Punkt erscheint die UAC-Eingabeaufforderung. Wenn Sie Administratoranmeldeinformationen eingeben, verwendet Windows das Administratortoken, um das Programm zu

öffnen. Beachten Sie, dass auch alle Prozesse, die dieses erfolgreich erhöhte Programm seinerseits öffnet, ebenfalls als Administrator laufen.

Wenn eine Anwendung gestartet wird, die eine Privilegienanhebung benötigt, analysiert die UAC die Anwendung mit ihrer Anforderung und zeigt eine passende Eingabeaufforderung an. Als Administrator bekommen Sie meist eine Zustimmungs-Eingabeaufforderung zu sehen (Abbildung 7.11). (Und nein, es ist keine Einbildung: Dieses Dialogfeld sieht in Windows 10, Version 1607, völlig anders aus als in älteren Windows-Versionen.) Lesen Sie den Inhalt durch, prüfen Sie den Namen des Programms und klicken Sie auf *Ja*, wenn Sie überzeugt sind, dass dieses Programm sicher ist.

Abbildung 7.11 Wenn Sie auf *Weitere Details anzeigen* klicken, erscheint ein Link zum Zertifikat des Programms

Wenn Sie unter einem Standardkonto arbeiten, während Sie ein Programm starten, das eine Privilegienanhebung fordert, bekommen Sie eine Anmeldeinformationen-Eingabeaufforderung (Abbildung 7.12). Ist der Benutzer in der Lage, die Anmeldeinformationen (das heißt Benutzername und Kennwort, Smartcard oder biometrische Authentifizierung, abhängig davon, wie die Anmeldeauthentifizierung auf dem Computer konfiguriert ist) eines Administrators zur Verfügung zu stellen, wird die Anwendung mit dem Zugriffstoken eines Administrators ausgeführt.

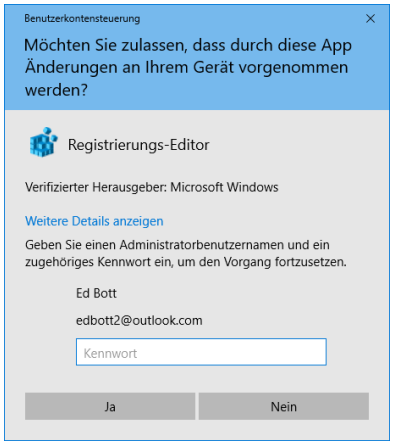

Abbildung 7.12 Will ein Standardbenutzer eine administrative Aufgabe ausführen, muss er das Kennwort für ein Administratorkonto eintippen

In der Standardeinstellung öffnet sich das UAC-Dialogfeld auf dem sicheren Desktop, der in einer separaten Sitzung läuft. Auf diese Weise ist sichergestellt, dass ein vertrauenswürdiger Prozess mit Systemprivilegien läuft. (Würde die UAC-Eingabeaufforderung in derselben Sitzung wie andere Prozesse laufen, könnte sich ein böswilliges Programm als UAC-Dialogfeld tarnen, etwa mit einer Meldung, die Sie auffordert, das Programm fortzusetzen. Ein böswilliges Programm könnte auch Ihre Tastatureingaben abfangen und so Ihr Administratorkennwort ausspähen.) Während der sichere Desktop angezeigt wird, können Sie nicht zu einem anderen Programm wechseln oder ein Fenster auf dem Desktop anklicken. (Auf dem sicheren Desktop von Windows 10 bekommen Sie ohnehin weder die Taskleiste noch irgendwelche anderen offenen Fenster zu sehen. Wenn die UAC zum sicheren Desktop wechselt, zeigt sie lediglich eine abgedunkelte Version des aktuellen Desktophintergrunds hinter dem UAC-Dialogfeld an.)

TROUBLESHOOTING

Es gibt eine gewisse Verzögerung, bis der sichere Desktop erscheint

Auf manchen Systemen müssen Sie mehrere Sekunden warten, bis sich der Bildschirm verdunkelt und die UAC-Eingabeaufforderung auf dem sicheren Desktop erscheint. Es gibt keine einfache Methode, diese Wartezeit zu verkürzen, aber Sie können das Problem umgehen. Sie können nämlich in den Einstellungen der Benutzerkontensteuerung (beschrieben im nächsten Abschnitt, »Ändern der UAC-Einstellungen«) die Schutzebene heruntersetzen. Die Stufe unterhalb der Standardeinstellung bietet denselben UAC-Schutz (wenn auch mit einem geringen Risiko, dass Schadsoftware den Desktop entführt), verzichtet aber darauf, den Desktop auszublenden.

Hinweis

Wenn eine andere Anwendung als die Vordergrundanwendung eine Privilegienanhebung anfordert, unterbricht die UAC nicht Ihre Arbeit (also die Vordergrundanwendung) mit einer Eingabeaufforderung, sondern lässt die entsprechende Taskleistenschaltfläche blinken. Klicken Sie auf die Taskleistenschaltfläche, um die Eingabeaufforderung anzuzeigen.

Nach einer Weile neigt man dazu, Dialogfelder wegzuklicken, ohne sie wirklich zu lesen oder auch nur kurz darüber nachzudenken. Es ist aber wichtig, sich bewusst zu machen, dass die Bedrohungen für Ihren Computer echt sind und dass Aktionen, die eine UAC-Eingabeaufforderung auslösen, möglicherweise gefährlich sind. Wenn Sie wissen, was Sie tun, und beispielsweise eine Schaltfläche anklicken, um die Windows Update-Einstellungen zu ändern, können Sie das entsprechende Sicherheitsdialogfeld nach einem kurzen Blick bestätigen, sofern Sie sich überzeugt haben, dass es von der erwarteten Anwendung ausgelöst wurde. Aber wenn eine UAC-Eingabeaufforderung erscheint, ohne dass Sie es erwarten, sollten Sie innehalten, den Inhalt sorgfältig durchlesen und in Ruhe überlegen, bevor Sie Ihre Erlaubnis geben.

Ändern der UAC-Einstellungen

Sie können Ihre Einstellungen für die Benutzerkontensteuerung anzeigen und ihre Arbeitsweise ändern, indem Sie **uac** in das Suchfeld eintippen und auf *Einstellungen der Benutzerkontensteuerung ändern* klicken. Daraufhin öffnet sich das Fenster aus Abbildung 7.13.

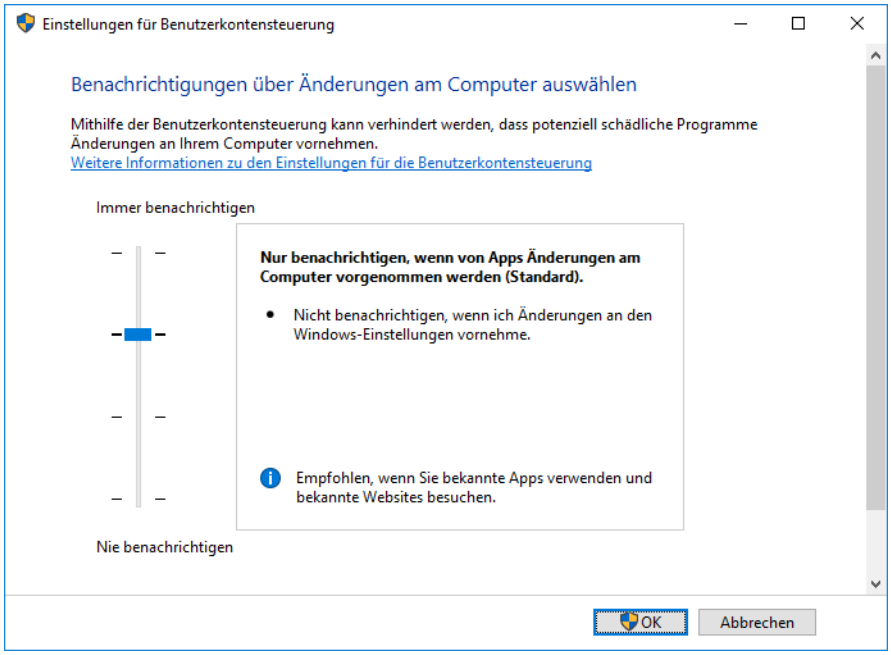

Abbildung 7.13 Sie sollten die Standardeinstellungen der Benutzerkontensteuerung nur ändern, wenn Sie genau durchblicken, welche Folgen dies hat

Welche Einstellungen Sie in diesem Fenster vorfinden, hängt davon ab, ob Sie ein Administrator- oder ein Standardkonto verwenden. Bei Standardkonten ist die oberste Stufe die Standardeinstellung, bei Administratorkonten dagegen die zweite Stufe von oben. Tabelle 7.1 fasst die verfügbaren Optionen zusammen.

Position des Schiebereglers	Bestätigungsaufforderung, wenn ein Programm versucht, Software zu installieren oder Änderungen am Computer vorzunehmen	Bestätigungsaufforderung, wenn Sie Änderungen an den Windows-Einstellungen vornehmen	Anzeige der Bestätigungsaufforderungen auf dem sicheren Desktop
Standardbenutzerkonto			
Oberste (Standard)	✓	✓	✓
Zweite	✓	✓	

Tabelle 7.1 Einstellungen für die Benutzerkontensteuerung

→

Position des Schiebereglers	Bestätigungsaufforderung, wenn ein Programm versucht, Software zu installieren oder Änderungen am Computer vorzunehmen	Bestätigungsaufforderung, wenn Sie Änderungen an den Windows-Einstellungen vornehmen	Anzeige der Bestätigungsaufforderungen auf dem sicheren Desktop
Dritte	✓		
Unterste (aus)			
Administratorkonto			
Oberste	✓	✓	✓
Zweite (Standard)	✓		✓
Dritte	✓		
Unterste (aus)			

Tabelle 7.1 Einstellungen für die Benutzerkontensteuerung (Forts.)

Sie ändern die Einstellungen, indem Sie den Schieberegler an die gewünschte Position bewegen. Lesen Sie sich den Hinweis durch, der unten im Feld angezeigt wird, während Sie den Schieberegler bewegen. Klicken Sie auf *OK*, wenn Sie fertig sind – und bestätigen Sie die UAC-Eingabeaufforderung, die an diesem Punkt erscheint! Wenn Sie mit einem Standardkonto angemeldet sind, können Sie die beiden untersten Stufen nicht auswählen, selbst wenn Sie das Kennwort für ein Administratorkonto besitzen. Um eine dieser Stufen auszuwählen, müssen Sie sich als Administrator anmelden und dann die Änderung durchführen.

TROUBLESHOOTING

Einstellungen für die Benutzerkontensteuerung bleiben nicht erhalten

Falls Sie feststellen, dass sich nichts ändert, wenn Sie eine Änderung an den Einstellungen für die Benutzerkontensteuerung vornehmen, sollten Sie sich überzeugen, dass Sie der Einzige sind, der momentan an Ihrem Computer angemeldet ist. Eine gleichzeitige Anmeldung, bei der die schnelle Benutzerumschaltung verwendet wird, kann dieses Problem verursachen.

Expertentipp

Passen Sie das UAC-Verhalten mithilfe der lokalen Sicherheitsrichtlinie an

Benutzer der Windows 10-Editionen Pro und Enterprise können das Verhalten der UAC mithilfe der Konsole *Lokale Sicherheitsrichtlinie* verändern. Starten Sie diese Konsole (*Secpol.msc*) und öffnen Sie den Zweig *Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen*. Sehen Sie sich in der Detailansicht die Richtlinien an, deren Namen mit dem Wort »Benutzerkontensteuerung« beginnen. Klicken Sie doppelt auf eine dieser Richtlinien und wechseln Sie zur Registerkarte *Erklärung*. Lesen Sie den Text durch, bevor Sie sich für eine Einstellung entscheiden. Mit diesen Richtlinien können Sie das Verhalten der UAC mit unterschiedlichen Methoden anpassen, darunter einigen, die im Fenster *Einstellungen für Benutzerkontensteuerung* nicht zur Verfügung stehen. (Administratoren in großen Unternehmensnetzwerken können diese Optionen auch über Gruppenrichtlinien-Verwaltungstools konfigurieren.) Einzelheiten zu diesen Richtlinien finden Sie im Artikel »UAC-Gruppenrichtlinien- und Registrierungsschlüsseleinstellungen« unter *https://bit.ly/uac-gpo*.

Unabhängig von Ihren UAC-Einstellungen werden die Schildsymbole auf jeden Fall in der Systemsteuerung angezeigt, aber Sie bekommen keine UAC-Eingabeaufforderungen angezeigt, wenn Sie den UAC-Schutz auf eine niedrige Stufe gesetzt haben. Wenn Sie eine Schaltfläche oder einen Link anklicken, der mit einem Schildsymbol markiert ist, beginnt sofort die entsprechende Aktion. Administratoren arbeiten mit vollständigen Administratorprivilegien, Standardbenutzer haben natürlich weiterhin nur Standardprivilegien.

Achtung

Vergessen Sie nicht, dass mehr hinter der UAC steckt als lästige Bestätigungsaufforderungen. Nur wenn die UAC aktiviert ist, arbeitet ein Administrator mit einem Standardtoken. Nur wenn die UAC aktiviert ist, läuft der Internet Explorer in einem geschützten Modus mit geringen Privilegien. Nur wenn die UAC aktiviert ist, werden Sie gewarnt, falls eine böswillige Anwendung versucht, eine Operation mit systemweiten Auswirkungen auszuführen. Und natürlich geht beim Deaktivieren der UAC auch die Datei- und Registrierungsvirtualisierung verloren, was Kompatibilitätsprobleme für Anwendungen auslösen kann, die vom UAC-Feature umgangen werden. Aus diesen Gründen raten wir dringend davon ab, die unterste Stufe in den Einstellungen für die Benutzerkontensteuerung zu wählen und damit die UAC vollständig auszuschalten.

Verschlüsseln von Daten

Windows stellt die folgenden Verschlüsselungstools zur Verfügung, um zu verhindern, dass vertrauliche Daten in die falschen Hände gelangen:

- Das verschlüsselnde Dateisystem (Encrypting File System, EFS) verschlüsselt Ihre Dateien so, dass selbst jemand, der sich die Dateien verschafft, sie nicht lesen kann. Die Dateien können nur gelesen werden, wenn Sie sich unter Ihrem Benutzerkonto am Computer anmelden.
- Die BitLocker-Laufwerkverschlüsselung bietet eine weitere Schutzschicht, indem sie gesamte Datenträgervolumes verschlüsselt. Wenn diese Verschlüsselung mit der

Speicherung des Schlüssels in einem TPM (Trusted Platform Module) kombiniert wird, verringert BitLocker die Gefahr, dass Daten missbraucht werden, wenn der ganze Computer geklaut wird oder eine Festplatte gestohlen und in einen anderen Computer eingebaut wird. Üblicherweise versucht ein Dieb in solchen Situationen, ein anderes Betriebssystem zu starten und die Daten vom gestohlenen Computer oder Laufwerk zu kopieren. Mit BitLocker ist diese Art von Offlineangriff zum Scheitern verurteilt.

- BitLocker To Go erweitert die BitLocker-Verschlüsselung auf Wechseldatenträger, zum Beispiel USB-Flashlaufwerke.

Hinweis

Verschlüsselndes Dateisystem und BitLocker-Laufwerkverschlüsselung stehen in Windows 10 Home nicht zur Verfügung. Wechseldatenträger können Sie nur dann mit BitLocker To Go verschlüsseln, wenn Sie Windows 10 Pro, Enterprise oder Education verwenden; ein auf diese Weise verschlüsseltes Laufwerk kann aber auch auf einem Gerät geöffnet werden, das unter Windows 10 Home läuft (es genügt eine beliebige Edition von Windows 7 oder neuer).

Arbeiten mit dem verschlüsselnden Dateisystem

Das verschlüsselnde Dateisystem (Encrypting File System, EFS) bietet eine sichere Methode, Ihre vertraulichen Daten zu speichern. Windows generiert einen zufälligen Dateiverschlüsselungsschlüssel (File Encryption Key, FEK) und verschlüsselt damit transparent die Daten, während sie auf den Datenträger geschrieben werden. Windows verschlüsselt den FEK dann mit Ihrem öffentlichen Schlüssel. (Windows erstellt ein persönliches Verschlüsselungszertifikat mit einem Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel, sobald Sie zum ersten Mal EFS nutzen.) Der FEK und somit die Daten, die er verschlüsselt, können nur mit Ihrem Zertifikat und dem zugehörigen privaten Schlüssel entschlüsselt werden. Und dieses Zertifikat steht nur zur Verfügung, wenn Sie sich mit Ihrem Benutzerkonto anmelden. (Zusätzlich können auch explizit festgelegte Datenwiederherstellungs-Agenten Ihre Daten entschlüsseln.) Andere Benutzer erhalten beim Versuch, auf Ihre verschlüsselten Dateien zuzugreifen, die Meldung »Zugriff verweigert«. Sogar Administratoren und andere, die über die Berechtigung verfügen, den Besitz über Ihre Dateien zu übernehmen, können die verschlüsselten Dateien nicht öffnen.

Sie können einzelne Dateien, ganze Ordner oder gesamte Laufwerke verschlüsseln. (Das Startvolume, auf dem sich die Windows-Betriebssystemdateien befinden, können Sie allerdings nicht mit EFS verschlüsseln. Dazu brauchen Sie BitLocker.) Wir empfehlen, dass Sie Ordner oder Laufwerke verschlüsseln, keine einzelnen Dateien. Wenn Sie einen Ordner oder ein Laufwerk verschlüsseln, werden alle darin bereits enthaltenen Dateien verschlüsselt, und künftig werden alle neuen Dateien, die Sie in diesem Ordner oder Laufwerk anlegen oder dorthin kopieren, automatisch verschlüsselt.

Gehen Sie folgendermaßen vor, um einen Ordner zu verschlüsseln:

1. Klicken Sie im Datei-Explorer mit der rechten Maustaste auf den Ordner, wählen Sie den Befehl *Eigenschaften*, klicken Sie auf die Registerkarte *Allgemein* und dort auf die Schaltfläche *Erweitert*. Daraufhin öffnet sich das Dialogfeld *Erweiterte Attribute* aus Abbildung 7.14. (Falls Sie im Eigenschaftendialogfeld nicht die Schaltfläche *Erweitert*

finden, liegt der Ordner nicht auf einem mit NTFS formatierten Volume. In diesem Fall steht EFS nicht zur Verfügung.)

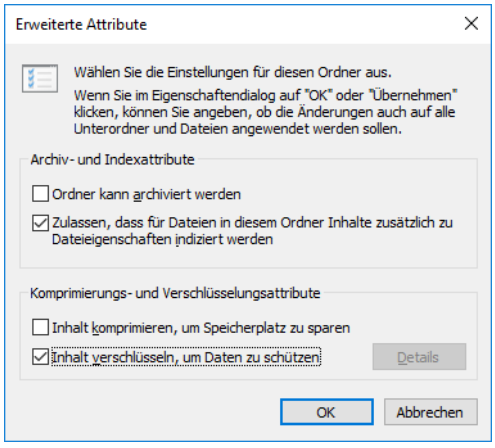

Abbildung 7.14 Verschlüsseln eines Ordners mit EFS

2. Aktivieren Sie das Kontrollkästchen *Inhalt verschlüsseln, um Daten zu schützen*. Beachten Sie, dass Sie keine komprimierten Dateien verschlüsseln können. Falls die Dateien bereits komprimiert sind, deaktiviert Windows die Komprimierung.
3. Klicken Sie zweimal auf *OK*. Falls der Ordner irgendwelche Dateien oder Unterordner enthält, fragt Windows nach, ob die Verschlüsselung durchgeführt werden soll (Abbildung 7.15).

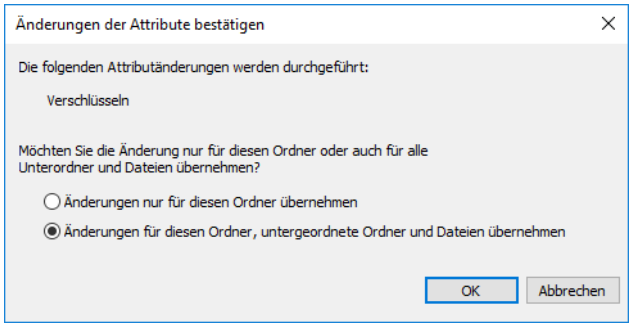

Abbildung 7.15 Die Verschlüsselung muss bestätigt werden, wenn ein Ordner bereits Dateien oder Unterordner enthält

Hinweis

Wenn Sie die Option *Änderungen nur für diesen Ordner übernehmen* wählen, verschlüsselt Windows keine Dateien, die momentan im Ordner abgelegt sind. Alle neuen Dateien, die Sie in diesem Ordner anlegen, werden allerdings verschlüsselt. Darunter fallen auch Dateien, die Sie in den Ordner kopieren oder verschieben.

Sobald eine Datei oder ein Ordner verschlüsselt wurde, zeigt der Datei-Explorer seinen Namen in grüner Schrift an. Dieser unscheinbare Hinweis ist üblicherweise die einzige Änderung, die Sie bemerken. Windows entschlüsselt Ihre Dateien im Hintergrund, sobald Sie darauf zugreifen, und verschlüsselt sie beim Speichern wieder.

Achtung

Bevor Sie etwas Wichtiges verschlüsseln, sollten Sie Ihr Dateiwiederherstellungszertifikat und Ihr persönliches Verschlüsselungszertifikat (mit den zugehörigen privaten Schlüsseln) sowie das Zertifikat des Datenwiederherstellungs-Agenten auf ein USB-Flashlaufwerk oder Ihr OneDrive speichern. Lagern Sie das Flashlaufwerk an einem sicheren Ort. Sie führen diese Datensicherung durch, indem Sie in der Systemsteuerung die Seite *Benutzerkonten* öffnen und auf *Dateiverschlüsselungszertifikate verwalten* klicken.

Falls die Zertifikate verloren gehen, die auf Ihrem Festplattenlaufwerk gespeichert sind (etwa wegen eines Datenträgerfehlers), können Sie die Sicherungskopie wiederherstellen und den Zugriff auf Ihre Dateien zurückerlangen. Wenn Sie alle Exemplare Ihres Zertifikats verlieren (und keine Zertifikate für Datenwiederherstellungs-Agenten vorhanden sind), wird es Ihnen nicht gelingen, Ihre verschlüsselten Dateien zu benutzen. Soweit wir wissen, gibt es keinen gangbaren Weg, ohne das Zertifikat auf diese verschlüsselten Dateien zuzugreifen. (Wäre das möglich, wäre es keine sonderlich gute Verschlüsselung.)

Um eine oder mehrere Dateien zu verschlüsseln, gehen Sie im Prinzip genauso vor wie bei Ordnern. Sie erhalten eine andere Bestätigungsnachricht, in der Sie daran erinnert werden, dass der Ordner, in dem die Datei liegt, nicht verschlüsselt ist, und das Angebot erhalten, ihn ebenfalls zu verschlüsseln. Im Allgemeinen ist es nicht sinnvoll, einzelne Dateien zu verschlüsseln, weil es dann zu einfach ist, die Daten, die Sie schützen wollen, ohne Ihr Wissen zu entschlüsseln. Zum Beispiel erstellen einige Anwendungen eine Kopie des ursprünglichen Dokuments, sobald Sie ein Dokument zum Bearbeiten öffnen. Wenn Sie das Dokument speichern, nachdem Sie fertig sind, speichert die Anwendung die Kopie – die unverschlüsselt ist – und löscht das ursprüngliche verschlüsselte Dokument. Unveränderliche Dateien, die Sie nur lesen, aber nie verändern, können Sie durchaus verschlüsseln, ohne auch den übergeordneten Ordner zu verschlüsseln. Aber sogar in dieser Situation ist es wahrscheinlich einfacher, den gesamten Ordner zu verschlüsseln.

Verschlüsseln mit BitLocker und BitLocker To Go

Mit der BitLocker-Laufwerkverschlüsselung können Sie gesamte NTFS-Volumes verschlüsseln, was hervorragenden Schutz gegen Datendiebstahl bietet. BitLocker kann ein Laufwerk vor Angriffen schützen, bei denen das Betriebssystem umgangen oder das Laufwerk ausgebaut und in einem anderen Computer angeschlossen wird. BitLocker bietet optimalen Schutz auf einem Computer, der mit einem TPM der Version 1.2 oder neuer ausgestattet ist. Auf solchen Systemen speichert das TPM den Schlüssel und stellt sicher, dass ein Computer nicht manipuliert wurde, während er ausgeschaltet war. Hat Ihr Computer kein TPM, können Sie BitLocker auf Ihrem Betriebssystemvolume trotzdem nutzen, sofern ein Administrator vorher die Gruppenrichtlinienoption *BitLocker ohne kompatibles TPM zulassen* eingeschaltet hat. In dieser Konfiguration müssen Sie dann aber jedes Mal, wenn Sie den Computer starten oder aus dem Ruhezustand aufwecken, den Startschlüssel auf einem

USB-Flashlaufwerk zur Verfügung stellen. Auf Systemen ohne TPM wird keine Systemdiagnose beim Start ausgeführt.

Mit BitLocker To Go, das in Windows 7 eingeführt wurde, können Sie den gesamten Inhalt eines USB-Flashlaufwerks oder eines anderen Wechseldatenträgers verschlüsseln. Wird er gestohlen oder verloren, ist der Dieb oder ein unehrlicher Finder nicht in der Lage, ohne das Kennwort auf die Daten zuzugreifen.

Sie wenden die BitLocker-Laufwerkverschlüsselung oder BitLocker To Go an, indem Sie im Datei-Explorer mit der rechten Maustaste auf das Laufwerk klicken und den Befehl *BitLocker aktivieren* wählen. BitLocker fragt Sie daraufhin, wie Sie das verschlüsselte Laufwerk entsperren wollen, das heißt mit einem Kennwort, einer Smartcard oder beidem. Sobald Sie die Methode gewählt und die Auswahl bestätigt haben, gibt Ihnen das System die Gelegenheit, Ihren Wiederherstellungsschlüssel zu speichern und auszudrucken (Abbildung 7.16).

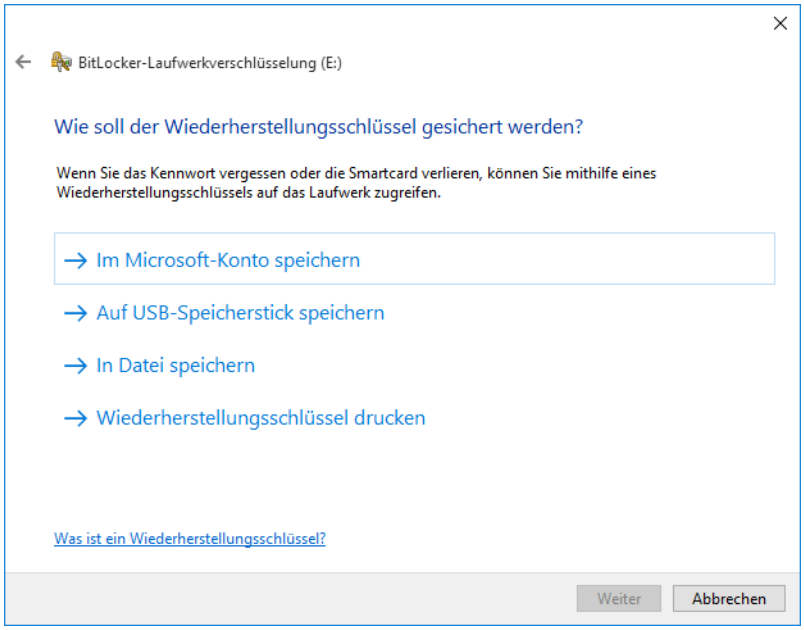

Abbildung 7.16 Windows 10 bietet die neue Möglichkeit, den Wiederherstellungsschlüssel in Ihrem Microsoft-Konto zu speichern

Ihr Wiederherstellungsschlüssel ist ein vom System generiertes, 48 Zeichen langes, numerisches Kennwort. Falls Sie das Kennwort für das verschlüsselte Laufwerk vergessen, können Sie Ihre Daten mit dem Wiederherstellungsschlüssel retten. BitLocker bietet an, diesen Schlüssel in einer Klartextdatei zu speichern. Sie sollten dieses Angebot wahrnehmen und die Datei an einem sicheren Ort ablegen.

Expertentipp

Speichern Sie Ihre Wiederherstellungsschlüssel auf OneDrive

Wenn Sie auf *Im Microsoft-Konto speichern* klicken, wird der Wiederherstellungsschlüssel auf Ihrem OneDrive gespeichert. Somit können Sie ein Verschlüsselungsproblem überall beseitigen, wo eine Internetverbindung besteht. Sie finden Ihren Schlüssel unter *https://onedrive.com/recoverykey*.

Nachdem alle Vorbereitungen abgeschlossen sind, beginnt BitLocker damit, Ihr Laufwerk zu verschlüsseln. Das dauert einige Minuten, sogar wenn das Laufwerk gerade erst frisch formatiert wurde. Wenn Sie es eilig haben, gibt es auch die Möglichkeit, lediglich den tatsächlich verwendeten Speicherplatz auf dem Laufwerk zu verschlüsseln. Diese Option kann Ihnen eine Menge Zeit sparen, wenn Ihr Laufwerk erst wenige Dateien enthält.

Um einen mit BitLocker verschlüsselten Wechseldatenträger zu lesen, müssen Sie ihn auf die Weise entsperren, die Sie beim Einrichten der Verschlüsselung konfiguriert haben. Falls Sie zur Eingabe eines Kennworts aufgefordert werden, es aber verloren oder vergessen haben, können Sie auf *Weitere Optionen* und dann auf *Wiederherstellungsschlüssel eingeben* klicken. Für den Fall, dass Sie mehrere Wiederherstellungsschlüssel-Textdateien haben, zeigt BitLocker To Go die Schlüssel-ID an (Abbildung 7.17).

Abbildung 7.17 Wenn Sie das Kennwort vergessen haben, können Sie einen mit BitLocker To Go verschlüsselten Wechseldatenträger mithilfe des Wiederherstellungsschlüssels entsperren

Suchen Sie den Eintrag auf OneDrive (*https://onedrive.com/recoverykey*) oder die Textdatei, deren Name zur Schlüssel-ID passt, und geben Sie den Wiederherstellungsschlüssel aus dieser Textdatei in das BitLocker-Dialogfeld ein. Nun erhalten Sie temporären Zugriff auf die Dateien, aber nur so lange, bis Sie den Datenträger wieder entfernen oder den Computer neu starten. An diesem Punkt ist es sinnvoll, das Kennwort zu ändern. Öffnen Sie dazu das Fenster *BitLocker-Laufwerkverschlüsselung* aus der Kategorie *System und Sicherheit* der Systemsteuerung, wählen Sie den verschlüsselten Wechseldatenträger aus und klicken Sie auf *Kennwort ändern*.

Sie können die BitLocker-Verschlüsselung eines Datenträgers beenden, indem Sie in der Systemsteuerung das Fenster *BitLocker-Laufwerkverschlüsselung* öffnen und auf *BitLocker deaktivieren* klicken. Die Software entschlüsselt daraufhin das Laufwerk, was einige Zeit dauern kann.

▶ **Weitere Informationen über BitLocker finden Sie unter *bit.ly/bitlocker-overview*.**

Blockieren von Schadsoftware mit Windows Defender

Am besten können Sie unerwünschte und böswillige Software bekämpfen, indem Sie verhindern, dass sie überhaupt auf einem PC installiert wird, der Mitglied Ihres Netzwerks ist. Im Lauf der Jahre haben Hacker viele Wege entwickelt, Schadsoftware zu installieren: Disketten, Dokumentdateien, E-Mail-Anhänge, Instant-Messaging-Anhänge, AutoPlay auf USB-Flashlaufwerken, Skripts, Browser-Add-Ons, die Liste ließe sich noch lange fortsetzen. Viele dieser Übertragungswege basieren auf Social-Engineering-Techniken, mit denen unachtsame oder leichtgläubige Benutzer dazu gebracht werden, einen infizierten Anhang zu öffnen, eine infizierte Website zu besuchen oder in eine andere Falle zu tappen. Nicht damit zufrieden, sich auf unaufmerksame oder leichtgläubige Leute zu beschränken, sind Autoren von Schadsoftware immer auf der Suche nach Techniken, mit denen sich Infektionen automatisch verbreiten.

Jedes Programm, das versucht, sich ohne Ihr Wissen und Ihre explizite Zustimmung auf Ihren PC einzuschleichen, sollte blockiert werden. Eine wichtige Maßnahme im Rahmen einer PC-Schutzstrategie besteht deshalb darin, Antischadsoftware-Programme einzusetzen und stets auf dem neuesten Stand zu halten. Vorhang auf für Windows Defender, das in Windows 10 enthaltene Antischadsoftware-Programm.

Windows Defender läuft als Systemdienst und greift auf eine Scanning-Engine zurück, um Dateien mit den Einträgen einer Datenbank aus Virus- und Spywaredefinitionen zu vergleichen. Zusätzlich wendet er eine heuristische Analyse auf das Verhalten von Programmen an, um auf verdächtige Aktivitäten einer Datei aufmerksam zu machen, selbst wenn sie nicht in der Liste bekannter Bedrohungen verzeichnet ist. Er prüft jede Datei, auf die Sie auf irgendeine Art zugreifen, seien es Downloads aus dem Internet oder E-Mail-Anhänge, die Sie erhalten. (Dieses Feature wird als *Echtzeitschutz* bezeichnet. Sie dürfen es nicht mit planmäßigen *Überprüfungen* verwechseln, die in regelmäßigen Abständen alle Dateien, die auf Ihrem Computer gespeichert sind, untersuchen, um Schadsoftware auszumerzen.)

Benutzen von Windows Defender

Im Allgemeinen brauchen Sie Windows Defender überhaupt nicht zu »benutzen«. Als Systemdienst arbeitet er unmerklich im Hintergrund. Sie bemerken ihn nur, wenn er eine infizierte Datei findet. In diesem Fall zeigt er eine oder mehrere Benachrichtigungen an, um Sie zu warnen.

Trotzdem ist es sinnvoll, wenn Sie sich ein wenig in dem Programm umsehen. Gehen Sie dazu in der Einstellungen-App auf die Seite *Update und Sicherheit/Windows Defender*. Hier finden Sie die am häufigsten benötigten Optionen. Indem Sie den Schalter *Echtzeitschutz* auf die Stellung *Aus* setzen, können Sie den Schutz zeitweise deaktivieren (was Sie nur kurz tun sollten und nur dann, wenn Sie sicher sind, dass keinesfalls Schadsoftware in Ihren PC eindringen kann, die andernfalls blockiert würde).

Zwei erweiterte Optionen auf dieser Seite sind besonders wichtig:

- Im Abschnitt *Ausschlüsse* können Sie angeben, welche Dateien, Ordner, Dateitypen (anhand der Erweiterung) oder Prozesse Windows Defender ignorieren soll. Das ist besonders nützlich für Entwickler, wenn sie mit Dateien arbeiten, die andernfalls einen Windows Defender-Alarm auslösen würden.
- Der Abschnitt *Windows Defender Offline* ist neu in Windows 10, Version 1607. Wenn Sie auf die Schaltfläche in diesem Abschnitt klicken, wird der Computer neu gestartet und mit der Offline-Version von Windows Defender überprüft. Diese Technik ist nützlich, um hartnäckige Infektionen zu beseitigen, die in der Lage sind, sich der Echtzeiterkennung und -beseitigung zu entziehen.

Details darüber, was Windows Defender zuletzt getan hat, erhalten Sie, indem Sie auf *Windows Defender öffnen* klicken. Daraufhin öffnet sich die Konsole *Windows Defender* (Abbildung 7.18). Die Registerkarte *Startseite* zeigt den aktuellen Status und die Ergebnisse der letzten Überprüfung an. Auf dieser Registerkarte erfahren Sie auch, ob der Echtzeitschutz aktiviert ist.

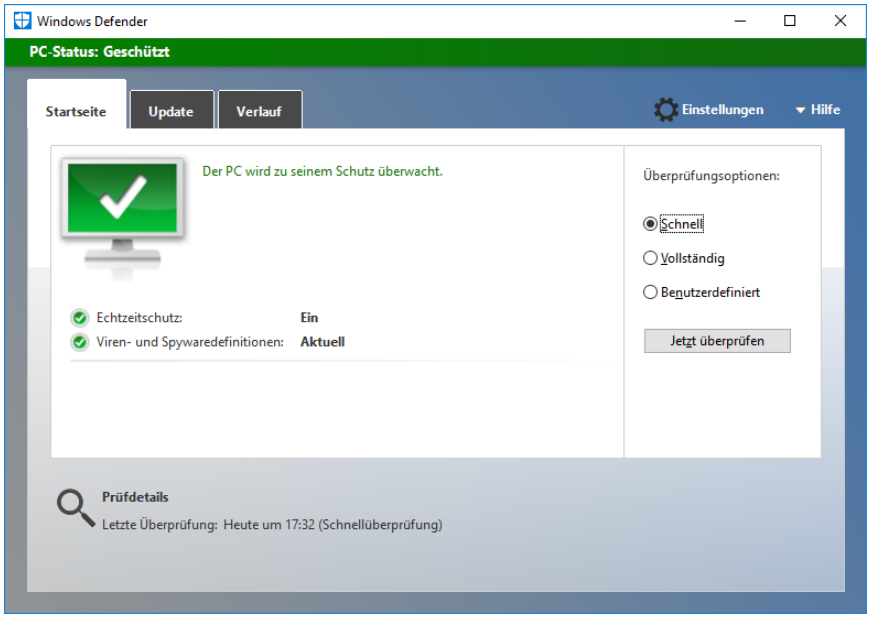

Abbildung 7.18 Die Registerkarte *Startseite* bietet einen Überblick über den Status von Windows Defender. Falls irgendeine Bedrohung Ihrer Aufmerksamkeit bedarf, färbt sich der Hintergrund gelb oder rot.

Manuell nach Schadsoftware suchen

Die Kombination aus Echtzeitschutz und regelmäßig geplanten Überprüfungen reicht normalerweise aus, um Probleme mit Schadsoftware und Spyware zu analysieren und zu beseitigen. Wenn Sie allerdings vermuten, dass Sie infiziert wurden, können Sie eine Überprüfung von Hand auslösen. Wählen Sie dazu auf der Registerkarte *Startseite* (Abbildung 7.18) unter *Überprüfungsoptionen* den gewünschten Typ aus und klicken Sie auf *Jetzt überprüfen*.

Die Option *Schnell* löst eine Überprüfung aus, die nur die Orte auf Ihrem Computer untersucht, in denen sich Schadsoftware und Spyware wahrscheinlich einnisten. Diese Option wird für häufige, regelmäßige Überprüfungen empfohlen. Wählen Sie die Option *Vollständig*, wenn Sie eine Infektion vermuten (oder sich lediglich überzeugen wollen, dass Ihr System sauber ist) und alle laufenden Programme sowie den vollständigen Inhalt aller lokalen Volumes überprüfen wollen. Schließlich können Sie noch die Option *Benutzerdefiniert* wählen, wenn Sie die Überprüfung auf eine bestimmte Kombination von Laufwerken, Ordnern und Dateien einschränken wollen.

Expertentipp

Ausführen einer Überprüfung aus einem Skript oder einer geplanten Aufgabe

Windows Defender umfasst ein Befehlszeilenprogramm, mit dem Sie Überprüfungen aus einem Skript oder einer geplanten Aufgabe heraus automatisieren können. Sie finden *MpCmdRun.exe* im Ordner *%ProgramFiles%\Windows Defender*. Einzelheiten über den Aufruf dieses Dienstprogramms erhalten Sie, wenn Sie eine Eingabeaufforderung mit erhöhten Rechten öffnen und das Programm ohne Argumente aufrufen.

Behandeln von erkannten Bedrohungen

Wenn der Windows Defender im Rahmen seines Echtzeitschutzes auf Schadsoftware oder Spyware stößt, zeigt er im Info-Center ein Banner sowie eine Benachrichtigung an und beseitigt das Problem in den meisten Fällen, ohne dass Sie einen Finger zu krümmen brauchen.

Sie erfahren mehr über die Funde, indem Sie im Windows Defender auf die Registerkarte *Verlauf* klicken. Wählen Sie die Option *Unter Quarantäne gestellte Elemente* aus und klicken Sie auf *Details einblenden*. Windows Defender zeigt den Namen, die Warnstufe und das Erkennungsdatum für Elemente an, die unter Quarantäne gestellt wurden (Abbildung 7.19).

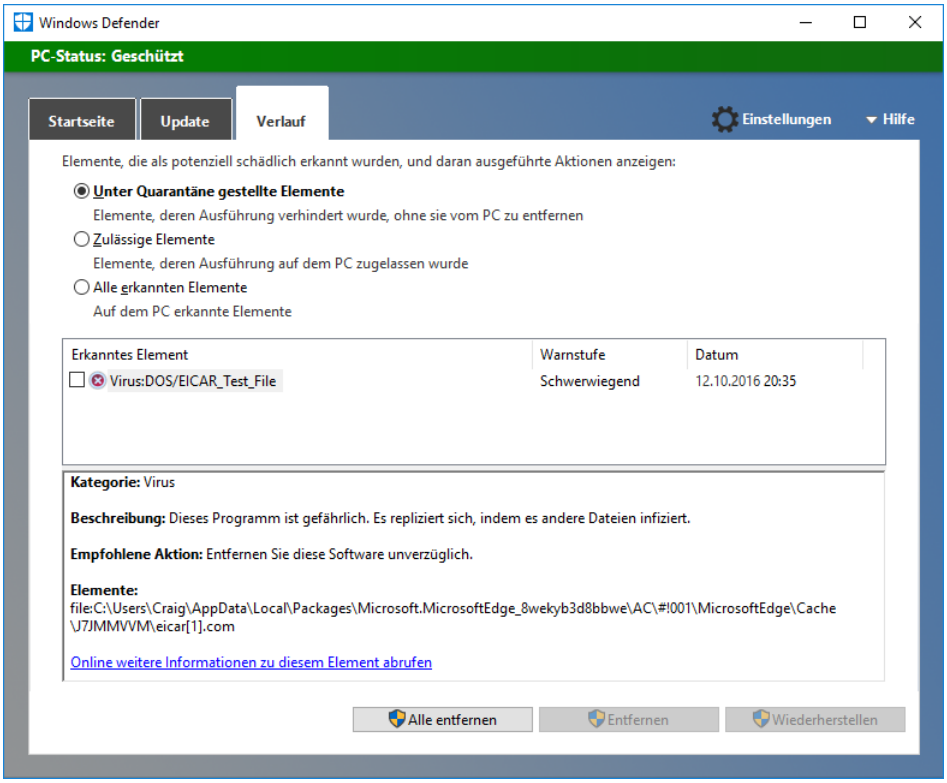

Abbildung 7.19 Das Feld unter der Liste zeigt Details über das ausgewählte Element an. Der Link ganz unten in diesem Feld führt zu Onlineinformationen über die erkannte Bedrohung.

Erkannte Elemente werden in den abgeschirmten Ordner *%ProgramData%\Microsoft\Windows Defender\Quarantine* verschoben, dessen Berechtigungen einen *Verweigern*-Zugriffssteuerungseintrag umfassen, der die vordefinierten Gruppen *Benutzer* und *Jeder* ausschließt. Ausführbare Dateien in diesem Ordner können nicht ausgeführt werden und es ist nicht möglich, mit dem Datei-Explorer auf den Inhalt des Ordners zuzugreifen. Hierher verschobene Elemente können nur in der Windows Defender-Konsole (empfohlen) oder in einer Eingabeaufforderung mit erhöhten Rechten verwaltet werden.

Stoppen unbekannter oder böswilliger Programme mit SmartScreen

Das in Windows 7 als Internet Explorer-Feature eingeführte SmartScreen identifiziert Programme, die von anderen Benutzern ohne Probleme ausgeführt wurden. Dazu vergleicht es den Hashwert eines heruntergeladenen Programms mit der Microsoft-Datenbank für Anwendungseinstufung. (Es überprüft auch Webinhalte, die von Windows Store-Apps benutzt werden.)

Diese Prüfung findet statt, wenn Sie ein Programm mit Microsoft Edge oder Internet Explorer herunterladen. SmartScreen wird außerdem aktiv, wenn Sie versuchen, ein Programm auszuführen, das Sie aus dem Internet heruntergeladen haben – ganz unabhängig davon, welchen Browser Sie einsetzen.

Programme mit positiver Einstufung laufen ohne Behinderung. Programme, die als schädlich bekannt sind oder noch keine Einstufung haben, werden blockiert. Dabei erscheint eine Meldung, die erst einmal nur mitteilt, dass SmartScreen den Start einer App verhindert hat (Abbildung 7.20).

Abbildung 7.20 Wenn Sie versuchen, ein heruntergeladenes Programm auszuführen, das nicht in Microsofts Datenbank verzeichnet ist, erscheint eine solche Meldung

Sofern Sie überzeugt sind, dass das Programm ungefährlich ist, können Sie die Sperre umgehen, indem Sie auf die Schaltfläche *Trotzdem ausführen* klicken. In den Standardeinstellungen muss jemand mit einem Administratorkonto zustimmen, dass das Programm ausgeführt werden darf. Sagen Sie nicht, Sie wurden nicht gewarnt.

Sie können den SmartScreen-Schutz ausschalten, indem Sie das Fenster *Sicherheit und Wartung* öffnen (siehe Abbildung 7.1 am Anfang dieses Kapitels) und auf *Windows SmartScreen-Einstellungen ändern* klicken.