Windows 11
Das Praxisbuch

DIE LESEPROBE

19 Schützen Sie sich gegen Angriffe aus dem Netz

Eine Firewall gehört schon seit einigen Jahren zum Lieferumfang von Windows. Das ist auch sinnvoll, denn eine solche Schutzfunktion bietet zwar keine vollkommene Sicherheit, aber einen guten Basisschutz. Da eine Firewall an sich ein recht komplexes Instrument ist, das in den Detaileinstellungen zumindest Grundwissen über Netzwerke erfordert, hat Microsoft die Windows Defender Firewall quasi zweigeteilt. Wer einfach nur sichere Einstellungen ohne viel Aufwand haben möchte, kann die Firewall mit einigen wenigen Grundeinstellungen in seinem Sinn konfigurieren. Wer aber in die Details gehen und spezifische Einstellungen für besondere Szenarien konfigurieren will, kann in den erweiterten Einstellungen sozusagen an jeder kleinen Schraube selbst drehen.

19.1 Die klassische Windows-Firewall für zuverlässigen Basisschutz

Angesichts der Gefahren im Internet ist eine Firewall eine unerlässliche Maßnahme. Sie filtert unerwünschte und potenziell gefährliche Pakete und Anfragen aus dem Datenstrom heraus und verhindert so, dass sie auf den PC gelangen. So werden die Zugänge des PCs vor unerwünschten Gästen geschützt, und auch bösartige Angriffe wie Portscans und Denial-of-Service-Attacken werden abgewehrt. Windows bringt hierfür einen Basisschutz in Form seiner klassischen Windows Defender Firewall mit.

Sichere Basiskonfiguration der Firewall

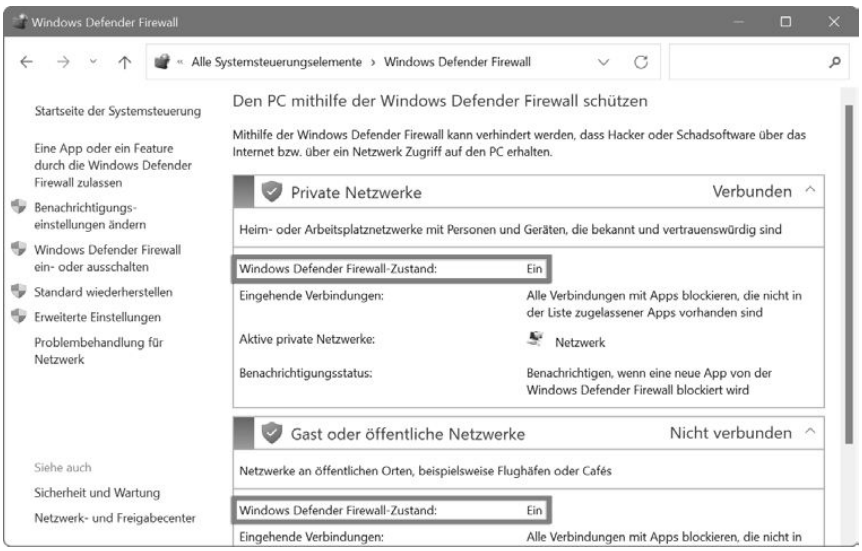
Die Windows Defender Firewall kann für jegliche Arten von Internetverbindung verwendet werden. Dabei spielt es keine Rolle, ob es sich um eine Einwählverbindung, einen DSL-Zugang über ein lokales Netzwerk oder auch um ein Drahtlosnetzwerk handelt. Die Firewall-Einstellungen können auf die jeweilige Rechner- und Zugangskonfiguration und das persönliche Sicherheitsbedürfnis abgestimmt werden. Hierzu unterscheidet die Firewall – wie auch das Netzwerk- und Freigabecenter – grundsätzlich zwei Arten von Netzwerken:

- Das sind zum einen **private Netzwerke** zu Hause oder an einem Arbeitsplatz, wo der PC mit anderen, prinzipiell vertrauenswürdigen PCs verbunden ist. Standardmäßig sind hier der Datenaustausch und das Teilen von Ressourcen möglich, und die Firewall-Einstellungen sind weniger restriktiv bzw. lassen problematische Aktivitäten ggf. nach einer Rückfrage zu.
- **Gast- oder öffentliche Netzwerke** wie z. B. offene WLAN-Hotspots oder Firmennetze, die von vielen Anwendern genutzt werden, behandelt Windows wesentlich restriktiver. Datenaustausch und Ressourcenfreigabe sind hier standardmäßig

nicht möglich. Eine vom öffentlichen Netzwerk bereitgestellte Internetverbindung kann selbstverständlich genutzt werden, unterliegt aber einer strengen Kontrolle bezüglich der Art der übertragenen Daten.

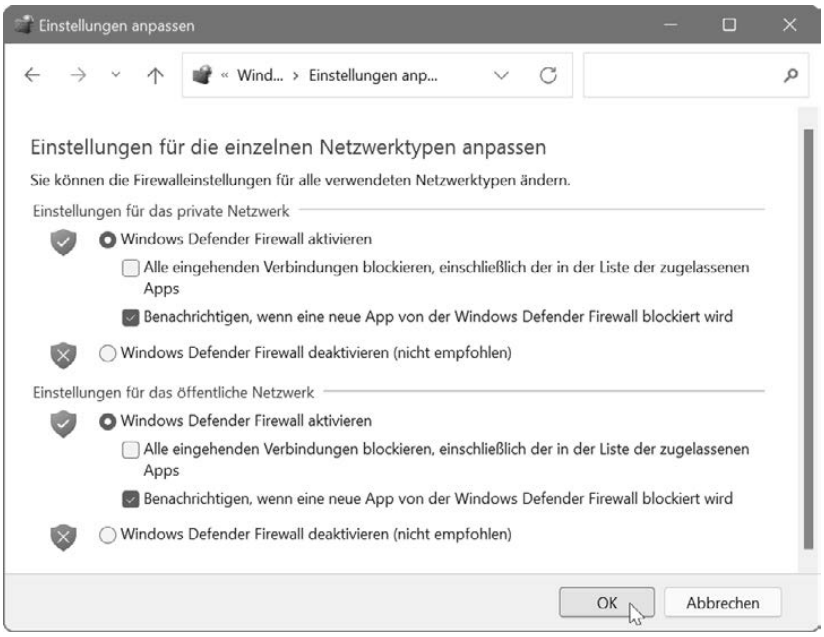
1. Um die Windows-Firewall einzustellen, öffnen Sie in der klassischen Systemsteuerung das Modul *Windows Defender Firewall*.

2. Im anschließenden Menü können Sie nun den aktuellen Status von Netzwerk und Firewall sowie die Grundkonfiguration der Firewall einsehen. Hier zeigt sich die Unterscheidung in private und öffentliche Netzwerke deutlich. Für jeden Bereich ist eine eigene Übersicht vorhanden, und Sie können dieselben – getrennten – Einstellungen für beide Arten von Netzwerken vornehmen.



3. Um die Konfiguration der Firewall zu verändern, klicken Sie links auf *Windows Defender Firewall ein- oder ausschalten*. So öffnen Sie die eigentlichen Firewall-Einstellungen. Auch hier ist alles zweigeteilt, und alle Einstellungen können separat für geschlossene und öffentliche Netze vorgenommen werden:

   - Standardmäßig ist die Schutzfunktion mit *Windows Defender Firewall aktivieren* eingeschaltet und läuft mit Basisregeln, die die üblichen Internetanwendungen zulassen. Nicht angeforderte Datenpakete von anderen Rechnern werden dabei verworfen, wenn diese nicht ausdrücklich als Ausnahmen definiert sind. Somit sind Sie vor Portscans, Trojanern etc. schon recht gut geschützt.
   - Insbesondere für mobile PCs, die hin und wieder an öffentlichen Netzwerken wie z. B. WLANs betrieben werden, ist die Option *Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste der zugelassenen Apps* gedacht. Sie ignoriert auch definierte Ausnahmeregeln und bietet so noch mehr Schutz.



- Die Option *Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird* setzt Sie davon in Kenntnis, wenn die Firewall aktiv ins Geschehen eingreift. Das kann sinnvoll sein, da ansonsten Anwendungen mit Internetzugriff nicht funktionieren und Sie nicht erfahren, warum das so ist. Sollten die Meldungen der Firewall nervig sein, können Sie sie aber so unterdrücken.
- Die Firewall mit *Windows Defender Firewall deaktivieren* auszuschalten, empfiehlt sich nur, wenn Sie stattdessen andere, mindestens ebenbürtige Schutzmaßnahmen ergreifen.

4. Wenn Sie die geänderte Einstellung mit *OK* übernehmen, wird die Firewall-Funktion entsprechend Ihrer Auswahl eingestellt. Dies ist ohne Neustart möglich, sodass Sie den Modus auch während des Betriebs jederzeit schnell wechseln können.

Anwendungen den Internetzugang freigeben

Die Windows Defender Firewall überwacht nicht nur den von außen ankommenden Datenverkehr, sondern achtet auch auf Programme, die vom PC aus Daten ins Internet übertragen wollen. Schließlich könnte es sich dabei ja um Trojaner oder andere schwarze Schafe handeln. Nimmt ein Programm Kontakt mit dem Internet auf, vergleicht die Windows-Firewall dieses mit ihrer internen Liste und wird aktiv, wenn das Programm dort nicht verzeichnet oder gar gesperrt ist. Das kann freilich auch passieren, wenn Sie selbst eine Internetanwendung zum ersten Mal starten. Dann müssen Sie Windows beibringen, dieses Programm zu akzeptieren.

HINWEIS

Nachricht beim Blockieren von Programmen

Damit das interaktive Freischalten von Anwendungen für den Internetzugriff gelingen kann, muss in den Einstellungen der Windows-Firewall die Option *Benachrichtigen, wenn eine neue App von der Windows Defender Firewall blockiert wird* eingeschaltet sein (siehe vorangegangenen Abschnitt).

1. Wenn ein Programm auf das Internet zugreifen möchte, das die Windows Defender Firewall bislang nicht in der internen Liste verzeichnet hat, blockiert sie dessen Zugriff zunächst. Sie erhalten dazu ein Hinweisfenster.

2. Haben Sie dieses Programm selbst aufgerufen und wollen es online benutzen, können Sie zunächst wählen, ob der Zugriff nur in geschlossenen privaten Netzwerken oder auch an öffentlichen Hotspots erlaubt sein soll.

3. Klicken Sie dann unten auf *Zugriff zulassen*.

4. Wurde das Programm versehentlich gestartet oder handelt es sich um ein Programm, das gar keine Internetfunktionen haben sollte, oder haben Sie vielleicht gar kein Programm gestartet, klicken Sie unten rechts auf die Schaltfläche *Abbrechen*. Damit wird dieses Programm auf die rote Liste gesetzt.

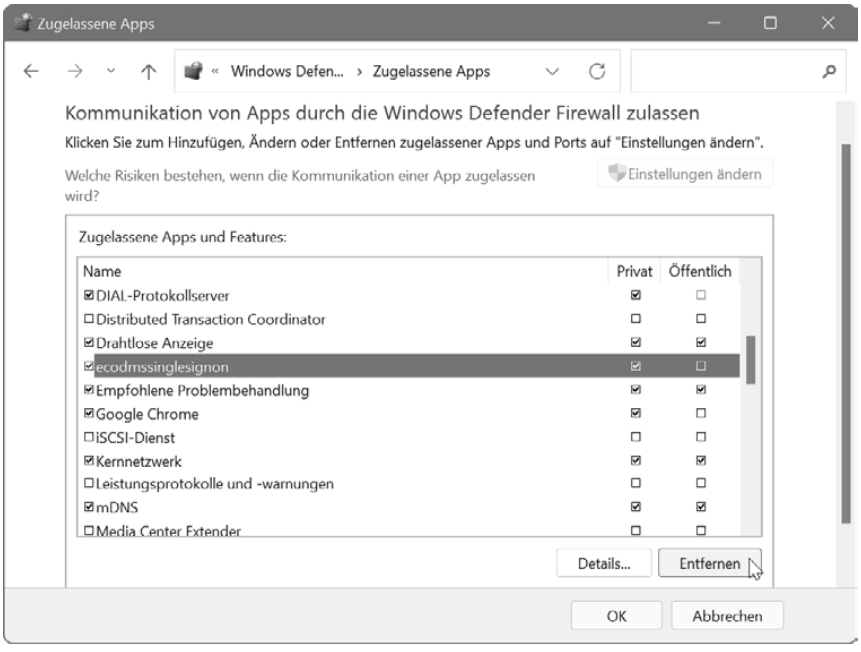
Die Zugangserlaubnis für ein Internetprogramm zurückziehen

Wenn Sie einem Internetprogramm den Zugriff aufs Internet gestattet haben, fragt Windows nicht mehr nach, sondern startet das Programm immer sofort. Das liegt daran, dass die Windows Defender Firewall alle Programme, denen Sie den Zugriff einmal erlaubt haben, in einer Liste speichert, um wiederholte Nachfragen zu vermeiden. Sie können ein Programm aber wieder aus dieser Liste streichen.

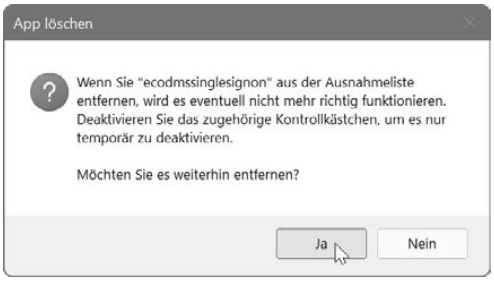
1. Öffnen Sie die *Windows Defender Firewall*-Einstellungen in der klassischen Systemsteuerung und klicken Sie dort links oben auf *Eine App oder ein Feature durch die Windows Defender Firewall zulassen*.

2. Klicken Sie im anschließenden Dialog zunächst oben auf die Schaltfläche *Einstellungen ändern*.

3. Suchen Sie in der Liste darunter einen Eintrag mit dem Namen des Programms. Wählen Sie diesen aus und klicken Sie dann ganz unten rechts auf die Schaltfläche *Entfernen*.



4. Bestätigen Sie die Sicherheitsrückfrage mit *Ja* und übernehmen Sie die Änderung schließlich mit *OK*. Beim nächsten Start dieser Anwendung fragt die Windows Defender Firewall wieder nach, und Sie können das Programm nun z. B. für den Internetzugang sperren.



HINWEIS

Internetanwendungen via Netzwerkports freischalten

Die Basiseinstellungen der Windows Defender Firewall sind komplett anwendungsorientiert. Freigaben können also immer nur für ein konkretes Programm ausgestellt werden. Sie können auch bestimmte Netzwerkports z. B. für VoIP-Internettelefonie, P2P-Tauschbörsen oder Instant Messaging freigeben, die dann von beliebigen Anwendungen genutzt werden können. Solche Einstellungen können aber nur in den erweiterten Einstellungen der Windows-Firewall vorgenommen werden (siehe im Folgenden).

19.2 Erweiterte Firewall-Einstellungen für flexiblen Schutz

Die Basisoptionen der Windows Defender Firewall lassen nur Grundeinstellungen sowie das Freigeben oder Sperren konkreter Anwendungen zu. Wer mehr will, muss sich mit den erweiterten Einstellungen beschäftigen. Deren Optionen und Möglichkeiten sind vielfältig und erfordern etwas mehr Kenntnisse als bei der klassischen Variante. Vor allem aber sind die Konfigurationsmöglichkeiten wohl etwas zu umfangreich und komplex, um sie als Symbol innerhalb der Systemsteuerung zu präsentieren. Deshalb führt der entsprechende Link Sie in die Tiefen der Computerverwaltung.

1. In den Basiseinstellungen der Windows Defender Firewall finden Sie diesen Link unter der Bezeichnung *Erweiterte Einstellungen*.

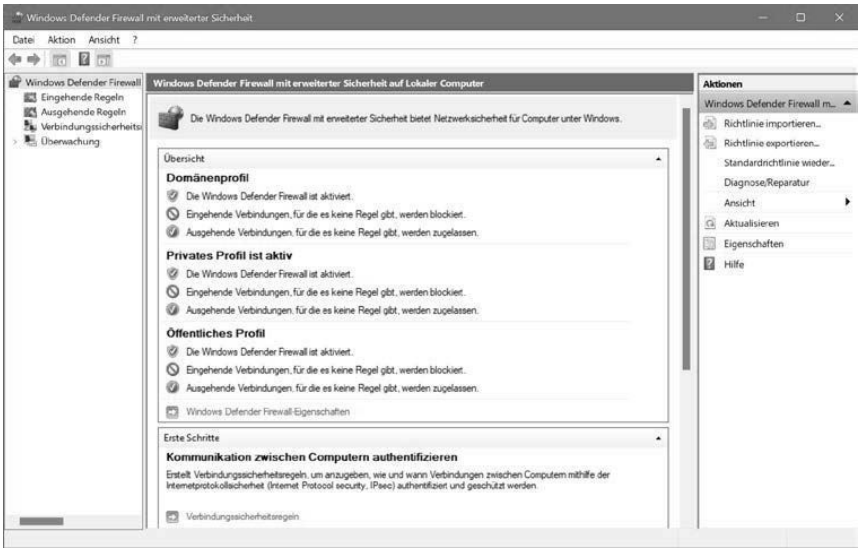
2. Damit gelangen Sie direkt in die auf den ersten Blick vielleicht etwas verwirrenden erweiterten Firewall-Einstellungen.

TIPP

Welches Profil ist das richtige?

Die erweiterte Windows Defender Firewall kann mit Einstellungen für verschiedene Szenarien versehen werden. Wenn Ihr PC mit einem Firmennetzwerk verbunden ist, das von einem Domänencontroller koordiniert wird, sind die Einstellungen unter *Domänenprofil* entscheidend. Für den klassischen Heim-PC, der allein steht oder nur mit einem kleinen lokalen Netzwerk verbunden ist, gelten die Einstellungen unter *Privates Profil*. Wenn Sie mit Ihrem PC an einem öffentlichen Netz teilnehmen, z. B. per WLAN in einem Internetcafé, werden die Einstellungen bei *Öffentliches Profil* verwendet. Die Optionen selbst unterscheiden sich nicht. Sie können aber verschiedene Einstellungen wählen, wenn der PC sich z. B. im Firmennetzwerk anders verhalten soll als zu Hause.

3. Im mittleren Bereich sehen Sie in der Übersicht die aktuellen Statusinformationen zur erweiterten Windows Defender Firewall. Achten Sie hierbei vor allem auf die Angaben zu dem Profil, bei dem *ist aktiv* vermerkt ist. Hier können Sie sehen, ob die Firewall derzeit aktiviert ist und wie sie mit eingehenden und ausgehenden Verbindungen standardmäßig umgeht.



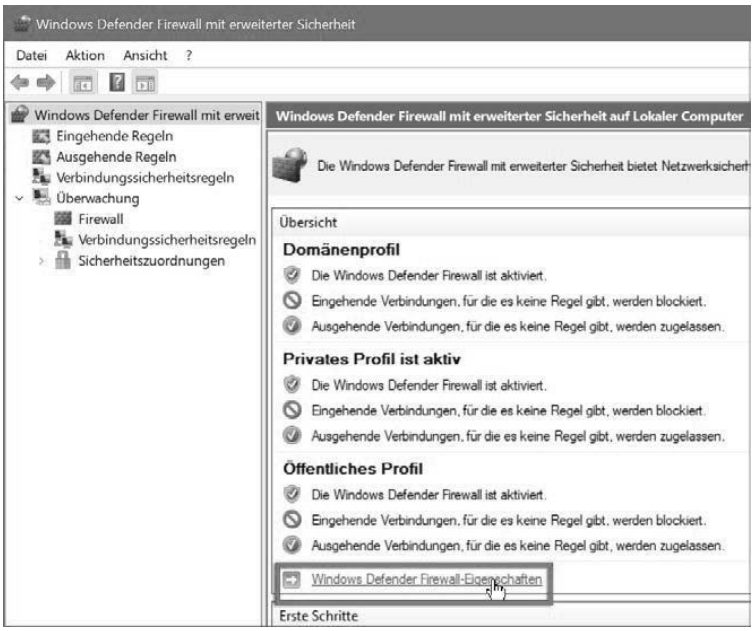
4. Weitere Informationen zur Firewall erhalten Sie über die Navigationsleiste ganz links. Dem Eintrag der Windows Defender Firewall ist ein Symbol vorangestellt. Genau wie in einer Ordnerleiste können Sie den Eintrag mit einem Klick darauf aufklappen und so weitere Unterbereiche zum Vorschein bringen, etwa die Listen mit den vordefinierten Ausnahmen für eingehende und ausgehende Datenverbindungen oder die Einstellungen zum Überwachen der Firewall.

5. Ganz rechts im Fenster sehen Sie die Leiste *Aktionen*. Diese ist kontextabhängig und verändert sich, wenn Sie links einen der Bereiche auswählen. Sie stellt jeweils die Funktionen zur Verfügung, die für die verschiedenen Bereiche relevant sind, wie z. B. das Anlegen neuer Ausnahmen. Außerdem finden Sie immer Funktionen zum Steuern der Ansicht sowie einen *Hilfe*-Link.

Die erweiterte Firewall konfigurieren

Die erweiterten Einstellungen der Windows Defender Firewall erlauben Ihnen wesentlich flexiblere und tiefer greifende Eingriffe in diese wichtigen Schutzmechanismen. Deshalb sollten Sie dabei auf eine sinnvolle Konfiguration achten, um die Netzwerkfunktionen Ihres PCs nicht zu beeinträchtigen.

1. Um die erweiterte Firewall einzustellen, wählen Sie links ganz oben den Eintrag *Windows Defender Firewall mit erweiterter Sicherheit* und klicken dann im mittleren Bereich im Abschnitt *Übersicht* ganz unten auf den Link *Windows Defender Firewall-Eigenschaften*.



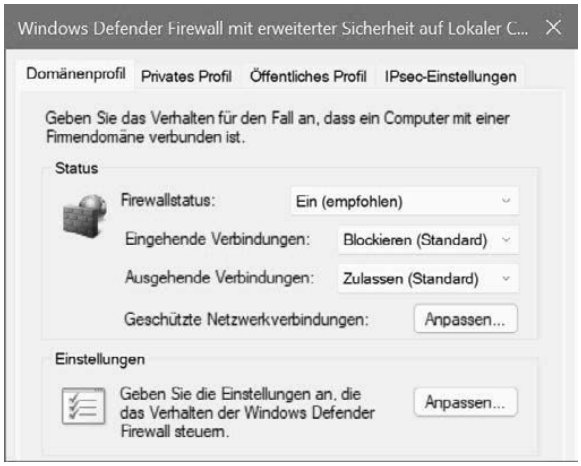
2. Damit öffnen Sie einen Einstellungsdialog, in dem Sie zunächst die richtige Registerkarte wählen sollten. Geht es um Einstellungen für ein öffentliches Netzwerk, sind Sie bei *Öffentliches Profil* richtig. Einstellungen für ein lokales, vertrauenswürdiges Netzwerk hingegen werden in *Privates Profil* konfiguriert. Inhaltlich sind beide Registerkarten identisch, deshalb ist an dieser Stelle etwas Umsicht erforderlich.

3. Um die Firewall zu aktivieren, setzen Sie das Auswahlfeld *Firewallstatus* auf *Ein*.

4. Danach sollten Sie unbedingt die Grundeinstellungen der Firewall überprüfen und ggf. anpassen:

   - *Eingehende Verbindungen* legt fest, wie die Firewall mit Verbindungen umgeht, die von außerhalb an den Rechner herangetragen werden. Mit *Blockieren (Standard)* verhindert das Programm alle Verbindungen, die nicht vom PC selbst angefordert wurden und für die keine Ausnahmeregelungen beste-

hen. Mit *Alle blockieren* unterbinden Sie jegliche Datenpakete von außerhalb. Diese Einstellung verhindert aber unter Umständen Internetdienste wie P2P-Dateitausch, Messaging oder Internettelefonie. Auf keinen Fall empfehlenswert ist hier die Einstellung *Zulassen*, da Ihr PC damit wie das sprichwörtliche Scheunentor offen steht.



- Etwas anders sieht die optimale Einstellung bei *Ausgehende Verbindungen* aus. Hier ist *Zulassen (Standard)* die übliche Einstellung. Sie lässt alle Datenverbindungen zu, die vom PC selbst aus nach draußen abgehen. Nur wenn für bestimmte Programme, Protokolle oder Ports Einschränkungen festgelegt werden, unterbindet die Firewall diese Verbindungen. Mit *Blockieren* würden sämtliche abgehenden Verbindungen unterbunden, und Ihr PC wäre praktisch völlig von der Außenwelt isoliert. Das mag in manchen speziellen Situationen wünschenswert sein, in der Regel aber sicherlich nicht.

5. Klicken Sie anschließend noch im Bereich *Einstellungen* auf die Schaltfläche *Anpassen*.

6. Im nächsten Dialog können Sie das grundlegende Verhalten der Windows Defender Firewall mit einigen Optionen steuern.

7. Sehr wichtig ist der Eintrag *Benachrichtigung anzeigen* oben im Bereich *Firewalleinstellungen*. Ist er aktiviert, wird der Benutzer informiert, wenn eine Anwendung auf seinem PC eine Verbindung herstellt, um Daten von außerhalb zu empfan-

gen. Verfügt der Benutzer über Administratorrechte, kann er dann entscheiden, dies zuzulassen oder zu blockieren. Kommt es allerdings sehr häufig zu solchen Rückfragen, kann es hilfreich sein, diese Option zu deaktivieren. Dann gelten die in den Einstellungen festgelegten Standardregeln.

8. Klicken Sie dann zweimal auf *OK*, um die jeweiligen Dialoge zu schließen und die gewählten Einstellungen zu aktivieren.

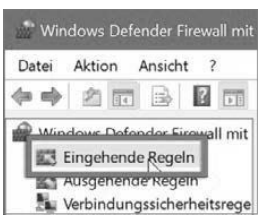
19.3 Firewall für wichtige Dienste durchlässig machen

Die Windows Defender Firewall filtert ein- und ausgehende Daten und lässt nur solche Pakete passieren, die zuvor von einer Anwendung oder einem Dienst des PCs ausdrücklich angefordert wurden. Beispiel: Wenn der Internet Explorer eine Webseite abruft, schickt er eine Anforderung an den entsprechenden Webserver. Dieser beantwortet sie mit den Daten der Webseite. Diese Antwort wird von der Firewall durchgelassen, da sie sich der Anforderung durch den Internet Explorer direkt zuordnen lässt. Es handelt sich also um erwünschte Daten.

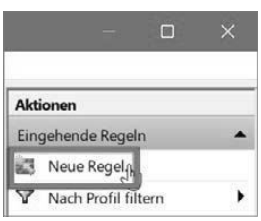
Datenpakete, zu denen sich keine Aufforderung direkt zuordnen lässt, werden hingegen blockiert. Auch hier ein vereinfachtes Beispiel: Bei der Internettelefonie per VoIP will Sie jemand erreichen. Dazu schickt sein VoIP-Programm ein entsprechendes Datenpaket an Ihren PC. Dieses wurde allerdings nicht ausdrücklich angefordert (denn Sie wissen ja nicht, dass jemand Sie jetzt gerade erreichen will).

Also blockiert die Firewall diese Daten, und Sie erfahren nichts von dem Anrufversuch. Daraus folgt nun nicht, dass sich Firewall und VoIP nicht vereinbaren lassen. Sie müssen aber in der Firewall eine Ausnahmeregel definieren, die Datenpakete mit VoIP-Anrufen grundsätzlich durchgehen lässt.

1. Wählen Sie in der Verwaltungskonsole der Firewall ganz links in der Navigationsleiste den Unterbereich *Eingehende Regeln*, in dem Sie Ausnahmeregeln für eingehende Datenverbindungen festlegen können.



2. Wechseln Sie dann auf die ganz rechte Seite des Fensters in den Bereich *Aktionen* und klicken Sie hier ganz oben auf *Neue Regel*. Damit starten Sie einen Assistenten, der Sie komfortabel durch die Schritte zum Definieren einer Firewall-Regel führt.



3. Wählen Sie im ersten Schritt, auf welcher Basis die Regel erstellt werden soll. Der Assistent kann Ausnahmeregeln an einem Programm, einem Port oder