

Zur Verfügung gestellt von
Mcert Deutsche Gesellschaft für IT – Sicherheit

Weitere Informationen unter www.mcert.de

Windows-Firewall

Version 1.0

Letzte Änderung: 21. Juli 2005

Impressum
Mcert Deutsche Gesellschaft für IT-Sicherheit mbH
Vertreten durch den Geschäftsführer Stefan Gehrke
Albrechtstraße 10
10117 Berlin

© 2005 Mcert GmbH

Das Werk wurde mit größter Sorgfalt erarbeitet. Dennoch können Fehler nicht ausgeschlossen werden. Es wird weder eine juristische Verantwortung noch eine Garantie für die Informationen und Abbildungen, weder ausdrücklich noch unausdrücklich, in Bezug auf Qualität, Durchführbarkeit oder Verwendbarkeit für einen bestimmten Zweck übernommen. In keinem Fall haftet Mcert Deutsche Gesellschaft für IT-Sicherheit mbH für direkte, indirekte oder gefolgte Schäden, die aus der Anwendung der Arbeit resultieren.

Im Folgenden Mcert Sicherheitstext wird beschrieben, was die Windows-Firewall ist, und welche Schutzfunktionen sie bietet. An Hand von Schritt-für-Schritt Anleitungen wird die Bedienung der Windows-Firewall erläutert.

Inhaltsverzeichnis

1. Einleitung

H1: Was ist eine Firewall?
H2: Welche Windows Version benutze ich?

2. Allgemeine Einstellungen

2.1. Der Windows-Firewall Dialog
2.2. Aktivieren der Windows-Firewall
2.3. Deaktivieren der Windows-Firewall
2.4. „Keine Ausnahmen zulassen“

H3: Administrator-Rechte
H4: Wann sollte die Windows-Firewall deaktiviert werden?
H5: Wozu dient der Modus „Keine Ausnahmen zulassen“?

3. Ausnahmen einrichten

3.1 Was tun, wenn eine Anwendung nicht funktioniert?
3.1.1. Ausnahmen über Programmnamen
3.1.2. Ausnahmen über Ports
3.2. Ausnahmen anzeigen und ändern

H6: Ausnahmen automatisch einrichten
H7: Bereich ändern
H8: Was sind Ports?

1. Einleitung

Eine Software-Firewall gehört mittlerweile zur Standard Sicherheits-Ausstattung eines Windows Computers. Sie wirkt praktisch als virtueller Schutzwall gegen direkte Angriffe aus dem Internet und blockt diese Attacken ab.

Solche Angriffe sind im Internet mittlerweile zur Regel geworden. Bei einem direkt mit dem Internet verbundenen Rechner vergeht meist keine Stunde, bevor die ersten Attacken den Computer treffen. Ohne Firewall wird Online-Zeit damit zum Risiko. Die Hauptursache für diese Angriffe sind automatisierte Bedrohungen, unter anderem die immer noch aktiven Internet-Würmer Sasser oder Blaster.

In Windows XP ist standardmäßig eine Firewall integriert, die mit dem **Service Pack 2** nochmals erweitert wurde. Dieser Text beschreibt die Funktionen dieser **Windows-Firewall** genannten eingebauten Schutzfunktion. Mcert empfiehlt dringend, auf Windows XP Computern das Service Pack 2 zu installieren, da diese Aktualisierung neben der verbesserten Firewall eine Menge neuer Sicherheitsfunktionen enthält. In diesem Text wird daher nicht auf ältere Versionen der Windows-Firewall eingegangen. Weitere Hinweise zum Service Pack 2 finden Sie im Mcert-Sicherheitstext „Neue Sicherheitsfunktionen im Windows XP Service Pack 2“.

<http://www.mcert.de/mcertpublic/pdfs/winxp-sp2.pdf>

Die Windows-Firewall wird mit der Installation des Service Packs 2 automatisch gestartet. Damit ist die Firewall unauffällig im Hintergrund aktiv, ohne dass der Anwender etwas davon merkt. Um aber mögliche Nebenwirkungen mit anderen Anwendungen zu beheben, oder auch nur bei Benutzer-Nachfragen der Firewall die richtige Entscheidung zu treffen, ist es hilfreich, die einzelnen Funktionen und Einstellmöglichkeiten der Firewall zu kennen. Dazu dient dieser Text. Zusätzlich kann man mit einigen beschriebenen Funktionen die Firewall-Schutzfunktionen noch weiter optimieren.

Probleme im Zusammenhang mit der Windows-Firewall treten in der Regel nur bei Programmen auf, die Netzwerk-Dienste für andere Computer bereitstellen. Anwendungen, bei denen die Netzwerk-Kommunikation vom Anwender initiiert wird (so genannte Client-Anwendungen, also Browser, E-Mail Programme usw.) funktionieren auch mit der Windows-Firewall problemlos, ohne dass der Anwender sich darum kümmern muss. Bei anderen Software-Applikationen, bei denen der Rechner praktisch als Server fungiert und andere Computern über das Netzwerk auf den Computer zugreifen (das wohl am weitesten verbreiteten Beispiel hierfür ist die Datei- und Druckerfreigabe), ist möglicherweise eine Interaktion des Anwenders notwendig. In einem solchen Fall hilft dieser Text weiter, indem er für die übliche Szenarien das Vorgehen erläutert.

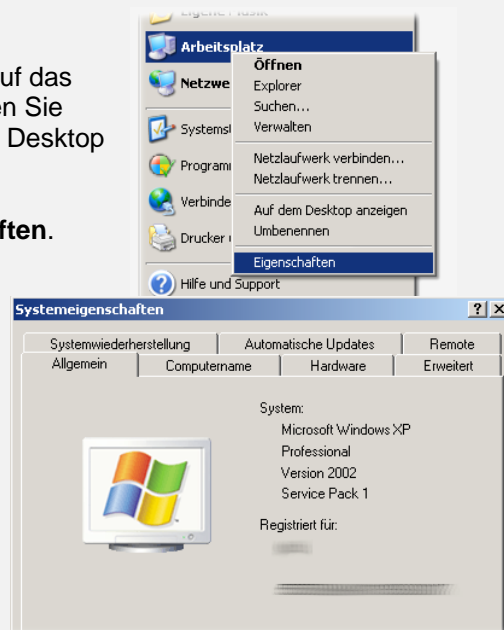
H1: Was ist eine Firewall?

Firewalls dienen im Allgemeinen dazu, Netzwerkanfragen zu filtern und zwischen erlaubtem und verbotenen Netzwerkverkehr zu unterscheiden. Dabei können Firewalls unterschiedlichste Formen annehmen, die Spannweite reicht von Software-Firewalls, die einen einzigen Computer schützen, über Firewalls in DSL-Routern, die ein Heim- oder kleines Firmennetz gegen Angriffe aus dem Internet schützen, bis hin zu teuren dedizierten Hardware-Firewalls, mit denen gleich mehrere große Netzwerke abgesichert werden und die vielfältige Schutzmöglichkeiten bieten.

Die Windows-Firewall ist als reine Computer-Anwendung eine Software-Firewall, auch Personal Firewall genannt, und schützt damit nur den Rechner, auf dem sie installiert ist.

H2: Welche Windows Version benutze ich?

1. Klicken Sie mit der *rechten* Maustaste auf das Symbol **Arbeitsplatz**. Das Symbol finden Sie entweder im **Start**-Menü oder auf Ihrem Desktop (Bildschirmhintergrund).
2. Wählen Sie den Menüpunkt **Eigenschaften**.
3. Im nun geöffneten Fenster **Systemeigenschaften** finden Sie auf der Startseite (Allgemein) die genaue Betriebssystem-Version unter **System**.



2. Allgemeine Einstellungen

2.1. Der Windows-Firewall Dialog

Die Einstellungen der Windows-Firewall lassen sich in dem Fenster **Windows-Firewall** vornehmen, das Sie über die folgenden Schritte erreichen:

1. Stellen Sie sicher, dass Sie Administrator-Rechte besitzen. (Siehe hierzu auch den Kasten **H3**.)
2. Klicken Sie im **Start-Menü** auf **Systemsteuerung**.

(Falls der Menüpunkt Systemsteuerung nicht im Start-Menü auftaucht, finden Sie ihn unter der Kategorie **Einstellungen** im Start-Menü.)

3. Klicken Sie im Fenster **Systemsteuerung** auf **Sicherheitscenter**.
4. Klicken Sie im **Sicherheitscenter-Fenster** unten auf den Eintrag **Windows-Firewall**.



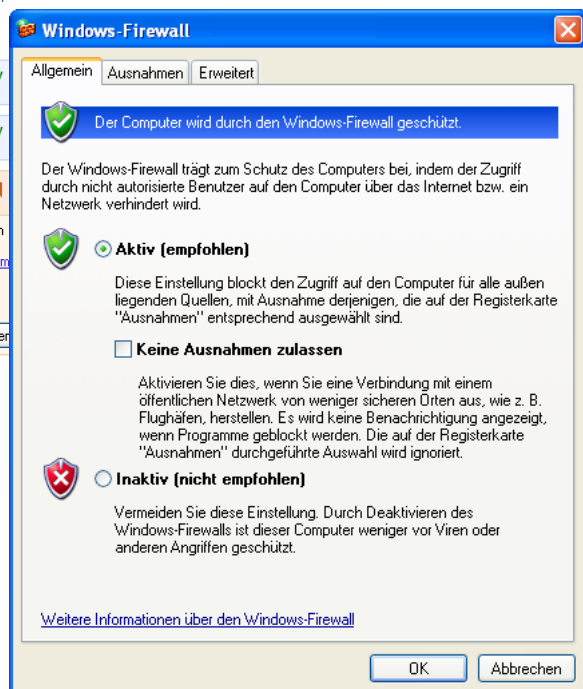
Wesentliche Sicherheitsmaßnahmen

Mit dem Sicherheitscenter können Sie Windows-Sicherheitseinstellungen verwalten. Stellen Sie sicher, dass die folgenden 3 wesentlichen Sicherheitsmaßnahmen aktiviert sind. Folgen Sie den Empfehlungen, wenn die Einstellungen nicht aktiviert sind. Öffnen Sie die Systemsteuerung, wenn Sie später zum Sicherheitscenter zurückkehren möchten.

[Neuheiten in Windows, die zum Schutz des Computers beitragen](#)



Sicherheitseinstellungen verwalten für:

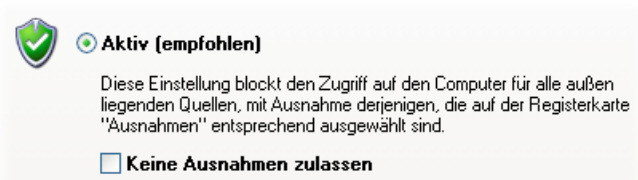


2.2. Aktivieren der Windows-Firewall

Die Windows-Firewall wird in Windows XP mit dem Service Pack 2 standardmäßig eingeschaltet. Falls Sie überprüfen wollen, ob die Windows-Firewall auf Ihrem Computer wirklich aktiv ist, oder sie nach dem Abschalten wieder aktivieren möchten, führen Sie die folgenden Schritte durch:

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.

2. Wählen Sie in den Windows-Firewall Einstellungen im Hauptfenster (Allgemein) die Option **Aktiv (empfohlen)**.



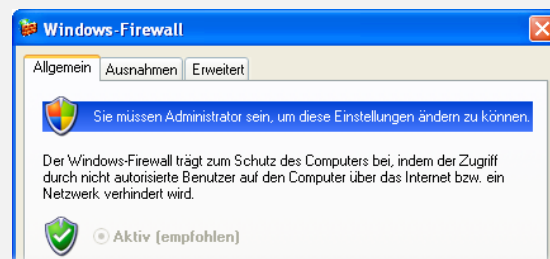
3. Klicken Sie auf **OK**.

H3: Administrator-Rechte

Besitze ich Administrator-Rechte?

Öffnen Sie die Windows-Firewall Einstellungen wie im Abschnitt 2.1 beschrieben (beginnen Sie bei Punkt 2).

- Falls im oberen Teil des Fensters der Hinweis erscheint **Sie müssen Administrator sein, um diese Einstellungen ändern zu können**, besitzt Ihr aktuelles Windows Benutzerkonto keine Administrator-Rechte.
- Falls stattdessen in dem blauen Balken ein anderer Text auftaucht, besitzen Sie bereits Administrator-Rechte.



Wie verschaffe ich mir Administrator-Rechte?

- Wenn Sie den Computer selbst eingerichtet haben und aus Sicherheitsgründen ein Benutzerkonto ohne Administrator-Rechte erstellt haben, melden Sie sich ab und melden Sie sich anschließend erneut unter dem Administrator-Benutzerkonto wieder an.
- Falls der Computer dagegen von einem Mitarbeiter oder Dienstleister betreut wird, oder Teil eines zentral administrierten Computernetzwerkes ist, sprechen Sie die verantwortliche Person auf Ihr Problem oder Ihren Änderungswunsch an.

2.3. Deaktivieren der Windows-Firewall

Warnung: Sie setzen Ihren Computer einem Risiko aus, wenn Sie ihn bei deaktivierter Firewall mit dem Internet verbinden! (Siehe hierzu auch Kasten H4.)

Um die Windows-Firewall vollständig zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.

2. Wählen Sie in den Windows-Firewall Einstellungen im Hauptfenster (Allgemein) die Option **Inaktiv (nicht empfohlen)**.



Inaktiv (nicht empfohlen)

Vermeiden Sie diese Einstellung. Durch Deaktivieren des Windows-Firewalls ist dieser Computer weniger vor Viren oder anderen Angriffen geschützt.

3. Klicken Sie auf **OK**.

H4: Wann sollte die Windows-Firewall deaktiviert werden?

Da die Windows-Firewall einen entscheidenden Sicherheitsvorteil gegen Angriff aus dem Netzwerk bietet, sollte sie nicht vorschnell abgeschaltet werden. Mögliche berechnete Gründe für das Deaktivieren der Windows-Firewall sind:

- Sie verwenden bereits eine Personal Firewall eines Drittanbieters.

Da andere Personal Firewalls denselben Schutz wie die Windows-Firewall bieten können, kann in diesem Fall die Windows-Firewall ohne Bedenken deaktiviert werden. Stellen Sie aber sicher, dass die Firewall des Drittanbieters wirklich aktiv und korrekt konfiguriert ist.

Sie sollten die Windows-Firewall jedoch **nicht** deaktivieren, wenn folgende Gründe vorliegen:

- Sie setzen den Computer nur in einem lokalen Firmen-Netzwerk ein, das vor Netzwerk-Angriffen scheinbar sicher ist.

Selbst in diesem Szenario sollte die Windows-Firewall aktiviert bleiben, da sich Internetwürmer wie Sasser oder Blaster auch in internen Netzwerken ausbreiten können, die relativ gut nach außen geschützt sind. So wurden interne Netzwerke von größeren Unternehmen bereits des Öfteren von solchen Schädlingen lahm gelegt, weil Mitarbeiter infizierte Laptops an das Unternehmens-Netzwerk angeschlossen haben. Sind in einem solchen Fall die internen Computer ungeschützt, haben Würmer leichtes Spiel.

- Sie verwenden eine Anwendung oder ein Programm, das durch die Windows-Firewall nicht mehr korrekt funktioniert.

Im nächsten Kapitel wird beschrieben, wie Sie die Einstellungen der Windows-Firewall so anpassen, dass Ihre Anwendung wieder funktioniert, ohne die Sicherheit des Computers zu gefährden.

2.4. „Keine Ausnahmen zulassen“

Mit der Option **Aktiv - Keine Ausnahmen zulassen** können Sie vorübergehend besonders sichere Firewall-Einstellungen herstellen (siehe hierzu Kasten **H5**).

Führen Sie folgende Schritte aus, um diesen Betriebsmodus zu aktivieren:

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.

2. Wählen Sie in den Windows-Firewall Einstellungen im Hauptfenster (Allgemein) die Option **Aktiv (empfohlen)**.



Aktiv (empfohlen)

Diese Einstellung blockt den Zugriff auf den Computer für alle außen liegenden Quellen, mit Ausnahme derjenigen, die auf der Registerkarte "Ausnahmen" entsprechend ausgewählt sind.

Keine Ausnahmen zulassen

Aktivieren Sie dies, wenn Sie eine Verbindung mit einem öffentlichen Netzwerk von weniger sicheren Orten aus, wie z. B. Flughäfen, herstellen. Es wird keine Benachrichtigung angezeigt, wenn Programme geblockt werden. Die auf der Registerkarte "Ausnahmen" durchgeführte Auswahl wird ignoriert.

3. Aktivieren Sie zusätzlich die Option **Keine Ausnahmen zulassen**.

4. Klicken Sie auf **OK**.

H5: Wozu dient der Modus „Keine Ausnahmen zulassen“?

Die Windows-Firewall bietet neben den einfachen Betriebsmodi **Aktiv** und **Inaktiv** noch einen weiteren Modus, der *sämtliche* Netzwerkanfragen von anderen Computern ablehnt. In diesem Zustand ist der Windows Computer bestmöglich gegen Angriffe geschützt, möglicherweise funktionieren damit aber nicht mehr alle Netzwerk-Anwendungen wie gewünscht.

Diese Option dient in erster Linie dazu, vorübergehend sehr restriktive Firewall-Einstellungen zu aktivieren, wenn sich ein Computer kurzzeitig in einem unsicheren Netzwerk befindet.

Ein **Beispiel** hierfür ist ein Firmen-Laptop, der die meiste Zeit im geschützten Unternehmens-Netzwerk verwendet wird. Damit Unternehmens-Anwendungen im Firmen-Netz korrekt funktionieren, mussten einige **Ausnahmen** in der Windows-Firewall eingerichtet werden, also die Firewall für bestimmte Dienste deaktiviert werden. Wird dieser Laptop nun z.B. von einem Mitarbeiter auch zu Hause eingesetzt und dort durch eine Modem-Verbindung direkt mit dem Internet verbunden, bieten diese Ausnahmen Angriffsflächen für Attacken aus dem Internet. Um diese Lücken zu schließen, kann der Laptop im Home-Office in den Betriebsmodus **Aktiv – Keine Ausnahmen zulassen** versetzt werden. Damit werden alle Ausnahmen deaktiviert und alle Netzwerk-Anfragen an den Computer abgelehnt. Client-Anwendungen wie Browser, E-Mail Programme und ähnliches funktionieren in diesem Modus aber weiterhin.

3. Ausnahmen einrichten

Die meisten Anwendungen arbeiten problemlos mit der Windows-Firewall zusammen und geben dem Benutzer die Möglichkeit, die Anwendung mit einem Klick an der Windows-Firewall frei zu schalten. In seltenen Fällen sind jedoch manuelle Anpassungen notwendig. Dies betrifft vor allem Serveranwendungen, also Programme, die anderen Computern in einem Netzwerk bestimmte Dienste bereitstellen. In solchen Fällen muss dieser Dienst in der Firewall freigegeben werden, damit andere Computer sich mit ihm verbinden können. Microsoft spricht hierbei von **Ausnahmen**, da einzelne Programme oder Dienste damit von Firewall-Schutz ausgenommen werden.

H6: Ausnahmen automatisch einrichten

Eine Ausnahme wird im einfachsten Fall selbständig bei der Installation einer Server-Anwendung eingerichtet. Das Installationsprogramm konfiguriert die Firewall-Änderung dabei automatisch, der Benutzer muss die Ausnahme eventuell noch bestätigen. Nach der Installation ist die Anwendung dann von anderen Computern erreichbar, ohne dass der Benutzer sich noch darum kümmern muss.

Falls eine Anwendung die Firewall-Ausnahme nicht bereits während der Installation einrichtet, wird der Benutzer in der Regel beim Start der Anwendung über eine **Windows Sicherheitswarnung** darauf hingewiesen, dass Netzwerkanfragen an diese Anwendung geblockt werden. In dem Fenster kann nun zwischen verschiedenen Aktionen ausgewählt werden:



- **Weiterhin blocken:**
Richtet keine neue Ausnahme für die Anwendung ein, und lehnt Netzwerkanfragen an den Dienst ab. Diese Einstellung wird permanent in die Firewall-Konfiguration eingetragen, so dass bei zukünftigen Starts der Anwendung nicht mehr erneut nachgefragt wird.
- **Nicht mehr blocken:**
Legt eine neue Ausnahme an, die für weitere Starts der Anwendung gültig bleibt, bis sie manuell geändert wird.
Die Option **Nicht mehr blocken** sollte nur dann ausgewählt werden, wenn Sie sicher sind, dass eine legitime Anwendung diese Warnung auslöst!
- **Erneut nachfragen:**
Hier wird ebenfalls keine Ausnahme eingerichtet, allerdings wird beim nächsten Start der Anwendung erneut nachgefragt.

Der Benutzer benötigt Administrator-Rechte, um ein Programm freizugeben. Besitzt er diese nicht, wird er in der Sicherheitswarnung darauf hingewiesen.

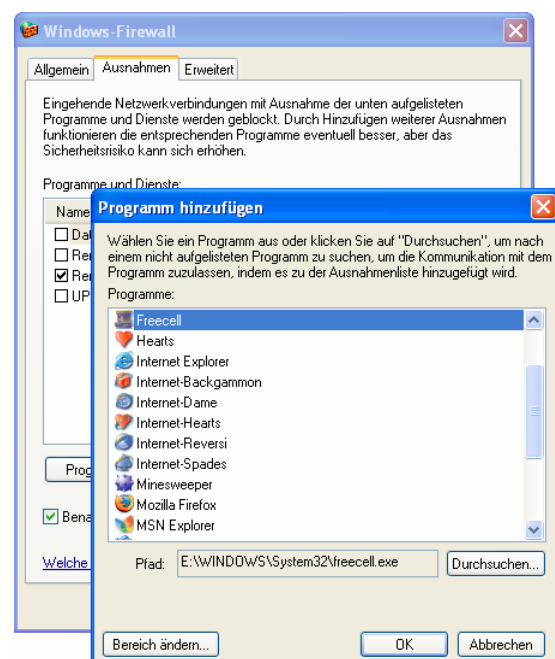
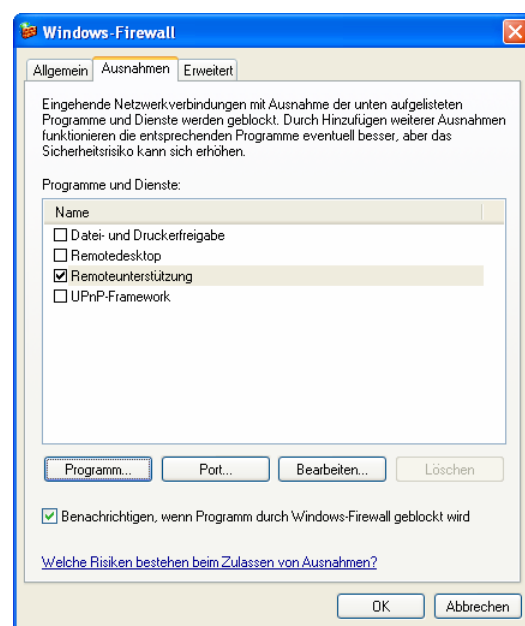
3.1. Was tun, wenn eine Anwendung nicht mehr funktioniert - Ausnahmen manuell einrichten

Falls eine Netzwerk-Anwendung nach Installation des Service Pack 2 nicht wie erwartet funktioniert, kann die Ursache dafür in einer Unverträglichkeit mit der Windows-Firewall liegen, die sich aber in der Regel leicht beheben lässt. Hinweise auf den Grund solcher potentiellen Probleme erhalten Sie z.B. über den Support des Herstellers.

Ist die Ursache die Windows-Firewall, kann das Programm manuell an der Firewall freigegeben werden. Die dazu nötigen Ausnahmen können über mehrere Mechanismen an der Windows-Firewall eingerichtet werden. Der bevorzugte Weg, eine Ausnahme zu konfigurieren, ist über **Programmnamen**. Falls das zu keinem Ergebnis führt, können auch Netzwerk-**Ports** angegeben werden.

3.1.1. Ausnahmen über Programmnamen

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.
2. Wählen Sie in den Windows-Firewall Einstellungen die Karteikarte **Ausnahmen**.
3. Klicken Sie auf **Programm...**
4. Wählen Sie aus der Liste das gewünschte Programm aus. Falls Sie die Anwendung in der Aufzählung nicht finden, klicken Sie auf **Durchsuchen...** und geben Sie den Ort der Anwendung an (üblicherweise unterhalb des Ordners C:\Programme\).
5. Als nächstes kann über die Option **Bereich ändern...** noch festgelegt werden, welche Computer auf den Dienst zugreifen dürfen. Wird diese Angabe nicht gemacht, so können alle Computer auf den Dienst zugreifen. (siehe dazu Kasten H7)
6. Verlassen Sie das Fenster **Programm hinzufügen** mit einem Klick auf **OK**.
7. Beenden Sie das **Windows-Firewall** Fenster ebenfalls mit **OK**.



H7: Bereich ändern

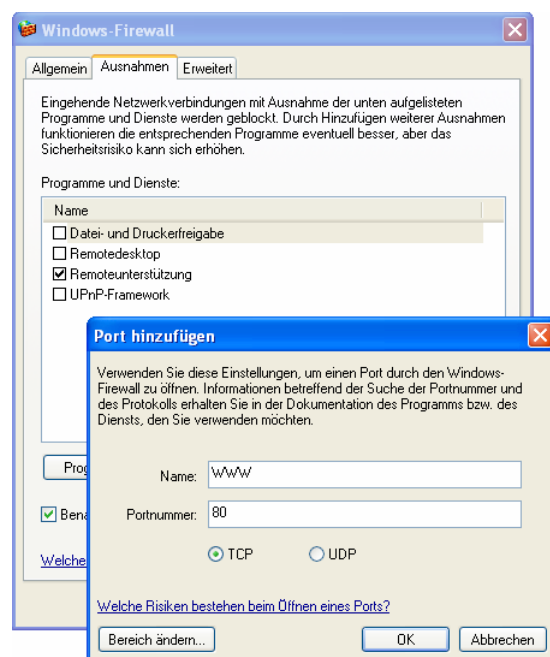
Mit der Option **Bereich ändern...** legen Sie fest, welche Computer im Netzwerk bei einer Ausnahme auf einen Dienst zugreifen können. Die drei Alternativen sind:

- Die Standard-Option ist **Alle Computer (einschließlich der im Internet)**. Da eine Anwendung durch diese Alternative von sämtlichen Computern im Internet zu erreichen ist, sollte geprüft werden, ob das wirklich erwünscht ist. Schnell werden so unbeabsichtigt Einfallstore für Hacker geöffnet oder interne Daten im Internet veröffentlicht.
- Oft reicht auch die zweite Option, **Nur für eigenes Netzwerk (Subnetz)**, die Computern außerhalb des lokalen Netzwerks den Zugriff auf den Dienst verbietet. Versuchen Sie aus Sicherheitsgründen zunächst, die Ausnahme mit dieser Option anzulegen – falls die Anwendung damit nicht zufrieden stellend arbeitet, können Sie problemlos nachträglich wieder auf die Standard-Option **Alle Computer (einschließlich der im Internet)** wechseln.
- Bei komplexeren Netzwerken erweist sich die dritte Option **Benutzerdefinierte Liste** als hilfreich. Hier kann eine ausführliche Liste von Netzwerkadressen und Netzwerken (Subnetzen) angegeben werden, von denen aus die Anwendung erreichbar sein soll.

3.1.2. Ausnahmen über Ports

Die zweite Möglichkeit, eine Ausnahme einzurichten, besteht in der Freigabe von bestimmten **Ports** (siehe hierzu Kasten **H8**). Falls die Freigabe für eine Anwendung über Netzwerk-Ports notwendig ist, finden Sie in den meisten Fällen Informationen dazu in der Dokumentation oder auf den Support-Webseiten des Herstellers. Insbesondere finden Sie dort meist Angaben, welche Portnummern für welches Protokoll (TCP oder UDP) freigegeben werden müssen. Haben Sie sich diesen Daten beschafft, gehen Sie wie folgt vor:

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.
2. Wählen Sie in den Windows-Firewall Einstellungen die Karteikarte **Ausnahmen**.
3. Klicken Sie auf **Port...**
4. Im Konfigurationsfenster **Port hinzufügen** kann der Ausnahme ein beliebiger Name, die Portnummer und das Protokoll (TCP oder UDP) zugeordnet werden.
5. Als nächstes kann über die Option **Bereich ändern...** noch festgelegt werden, welche Computer auf den Dienst zugreifen dürfen. Wird diese Angabe nicht gemacht, so können alle Computer auf den Dienst zugreifen. (siehe hierzu Kasten **H7**)



6. Verlassen Sie das Fenster **Port hinzufügen** mit einem Klick auf **OK**.
7. Schließen Sie das **Windows-Firewall** Fenster ebenfalls mit **OK**.

H8: Was sind Ports?

Anhand von Ports werden verschiedene Server-Dienste (also Programme, auf die andere Computer über das Netzwerk zugreifen können) unterschieden, die auf einem einzigen Computer angeboten werden. So kann z.B. ein Arbeitsgruppen-Server gleichzeitig Datei- und Druckerfreigaben, einen Webserver und Mailedienste anbieten. Um jeden dieser Dienste getrennt erreichen zu können, sind jedem Dienst eindeutige Portnummern zugeordnet. So wird der Webserver (HTTP) über die Portnummer 80/TCP identifiziert, der Dienst für den Mailversand (SMTP) über die Portnummer 25/TCP, der Dienst für die Namensauflösung (DNS) über die Portnummer 53/UDP usw. Wie in den Beispielen gezeigt, wird neben der Portnummer immer auch die Angabe des Protokolls (TCP oder UDP) benötigt, um einen Dienst auf einem Computer eindeutig zu adressieren.

Zur Verdeutlichung könnte man Portangaben mit Klingelschildern eines Hochhauses vergleichen. Obwohl alle Bewohner (in der Computer-Analogie: Dienste) dieses Hauses (Computers) dieselbe Adresse haben (Netzwerk-Adresse), sind sie doch einzeln über ihr eigenes Klingelschild erreichbar (Portangabe).

3.2. Ausnahmen anzeigen und ändern

Um bereits vorhandene Firewall-Ausnahmen anzuzeigen oder zu bearbeiten, öffnen Sie den **Ausnahmen**-Dialog im Windows-Firewall Fenster:

1. Öffnen Sie den Windows-Firewall Dialog wie in Abschnitt 2.1 beschrieben.
2. Wählen Sie in den Windows-Firewall Einstellungen die Karteikarte **Ausnahmen**.

Hier können Sie...

- sich einen Überblick über die vorhandenen Ausnahmen verschaffen.
- bereits **vorhandene Ausnahmen deaktivieren**, indem Sie den Haken vor dem Eintrag entfernen. Anschließend wird bei zugehörigen Programmen der Nutzer aber nicht benachrichtigt, wenn das Programm geblockt wird. Dies geschieht erst wieder, wenn der Ausnahme-Eintrag gelöscht wird.
- bereits **vorhandene Ausnahmen löschen**, indem Sie den gewünschten Eintrag markieren und auf **Löschen...** klicken.
- die Benachrichtigung bei Anwendungen ausschalten, die eine Ausnahme benötigen (siehe Kasten Ausnahmen **H6**), indem Sie den Haken **Benachrichtigung, wenn Programm durch die Windows-Firewall geblockt wird...** entfernen.
- in der Karteikarte **Erweitert** kann mit **Wiederherstellen** die Windows-Firewall auf die Standard-Konfiguration zurückgesetzt werden. Dabei gehen sämtliche bisher geänderten Einstellungen verloren.

Von Zeit zu Zeit empfiehlt es sich, die Liste der Ausnahmen auf unbekannte Einträge zu untersuchen. Verdächtig erscheinende oder unbekannte Ausnahmen sollten genauer untersucht werden. Eine Internet-Suche nach dem Namen des unbekanntes Eintrags hilft oft weiter, die Quelle des Eintrags zu identifizieren.

Um nicht unbeabsichtigt legitime Anwendungen zu beeinflussen, sollte eine solche verdächtige Ausnahme erst einmal deaktiviert werden. Treten keine Nebenwirkungen auf, kann der Eintrag später aus der Liste gelöscht werden.