
# Was ist eine Firewall?
# Bitdefender E-Guide

# Inhalt

Was ist eine Firewall? ..... 3
Wie eine Firewall arbeitet ..... 3
Welche Funktionen eine Firewall bieten sollte ..... 4
Einsatz von mehreren Firewalls ..... 4
Fazit ..... 5

Copyright © BitDefender 2012

Bitdefender

# Die Firewall – Ein unverzichtbarer Schutzwall für den PC

Heute ist es selbstverständlich, dass PCs, Notebooks, Smartphones und Tablet-Rechner auf das Internet zugreifen. Doch damit sind Risiken verbunden, speziell Angriffe von Hackern. Deshalb sind zwei Dinge auf jedem Rechner unverzichtbar: eine leistungsfähige Anti-Spyware-Lösung, Antivirenprogramme und eine Firewall.

## Was ist eine Firewall?

Die Hauptaufgabe einer Firewall besteht darin, Rechner oder Netzwerke vor unerwünschten Zugriffen aus dem Internet zu schützen. Außerdem lässt sich mit einer solchen Lösung steuern, mit welchen Servern oder Webseiten ein PC, Notebook oder Tablet-Rechner eine Verbindung aufbauen darf und welche Anwendungen dafür erlaubt sind.

Es gibt zwei Typen von Firewalls: Personal Firewalls, die auf einem Rechner installiert werden, und externe Firewall-Systeme. Personal Firewalls sind entweder im Betriebssystem eines Rechners integriert, etwa bei Windows und Mac OS, oder als separate Software erhältlich. In IT-Security-Lösungen führender Anbieter, wie etwa Bitdefender Internet Security 2013 oder Bitdefender Total Security 2013, ist eine Firewall bereits enthalten.

Speziell für Unternehmenskunden gibt es Firewall-Systeme, die aus einer Hardware-Plattform (Appliance) in Verbindung mit einer Firewall-Software bestehen. Diese Systeme sind vor allem für Unternehmensnetze mit vielen Arbeitsplatzrechnern gedacht. Zudem ist in den meisten DSL-Zugangssystemen wie DSL-Routern und kombinierten DSL-/WLAN-Routern eine Firewall integriert.

## Wie eine Firewall arbeitet

Die Firewall überprüft alle Datenpakete, die für einen Rechner oder ein Netzwerk bestimmt sind oder die von einem System aus ins Internet übermittelt werden. Anhand von Regeln, die der Nutzer oder Netzwerkverwalter vorgibt, entscheidet die Firewall, welche Datenverbindungen erlaubt sind. Dazu sperrt die Firewall "Ports" oder gibt diese frei. Ein Port ist eine Art Adresse, über die Datenpakete einem Netzwerk-Dienst zugeordnet werden. Jeder Netzwerk-Service nutzt spezielle Ports: E-Mail-Programme für die Übermittlung von Nachrichten über SMTP (Simple Mail Transfer Protocol) meist den Port 25, Browser für den Web-Zugriff Port 80.

Will ein Anwender verhindern, dass einzelne Netzwerkdienste Zugriff auf seinen Rechner erhalten, sperrt er die entsprechenden Ports. Deaktiviert er beispielsweise Port 23, kann kein externer User, auch kein Hacker, über Telnet "remote" auf seinen Rechner zugreifen. Umgekehrt hat ein Familienvater die Möglichkeit, auf dem PC im Kinderzimmer die Ports 6881 bis 6889 lahmzulegen und damit einen bekannten File-Sharing-Dienst (Azureus) auszusperren. So lässt sich verhindern, dass die Kinder illegale oder mit Schadprogrammen verseuchte Spielesoftware herunterladen.

Copyright © BitDefender 2012

## Welche Funktionen eine Firewall bieten sollte

Firewalls der Spitzenklasse, wie sie beispielsweise Bitdefender in seiner Produktline für private und Business-User integriert hat, zeichnen sich durch folgende Funktionen aus:

- **Umfassende Kontrolle des Internet-Verkehrs:** Der Nutzer kann detailliert festlegen, welche Anwendungen auf das Internet zugreifen dürfen beziehungsweise welche Applikationen Zugang zu seinem Rechner erhalten. Diese Regeln lassen sich anhand des Übertragungsprotokolls, Netzwerk-Ports, der Anwendungen oder IP-Adressen festlegen.
- **Alarm bei unzulässigen Aktionen:** Die Firewall muss alle unzulässigen oder verdächtigen Aktivitäten von Anwendungen unterbinden und den Nutzer darüber informieren. Dieser kann dann selbst entscheiden, ob er einer Applikationen den Zugriff auf das Internet oder einen Rechner erlaubt.
- **Datenbank mit internetfähigen Programmen**: Führende IT-Security-Anbieter wie Bitdefender erfassen in solchen Datenbanken "gute" Applikationen (White List) und solche, die von Cyber-Kriminellen lanciert werden. Solche bösartigen Anwendungen landen auf einer schwarzen Listen (Black List) und werden geblockt.
- **Schutz der Privatsphäre**: Auch seriöse Internet-Anwendungen nutzen Cookies. Dies sind Dateien, in denen ein Browser Details über die Internet-Nutzung des Anwenders speichert. Diese Informationen werden häufig an den Betreiber einer Web-Seite weitergeleitet, etwa damit dieser dem User beim nächsten Besuch der Web-Seite maßgeschneiderte Werbeangebote zukommen lassen kann. Firewalls sollten eine Funktion bieten, die auf Wunsch des Nutzers Cookies blocken und somit private Informationen schützen. Sollten Sie sich dennoch nicht sicher sein, ob Spyware oder Adware Ihren Computer bedroht, können Sie auch einen Virenscanner beauftragen Ihren PC genauer unter die Lupe zu nehmen.
- **Bidirektionale Absicherung aller Verbindungen:** Wichtig ist, dass die Firewall den Datenverkehr über alle Verbindungstypen absichert, und dies sowohl bei eingehenden als auch ausgehenden Connections. Gleich, ob ein Nutzer zu Hause oder am Arbeitsplatz mit seinem PC ins Internet geht oder unterwegs ein Notebook mit Wireless-LAN-Verbindung nutzt, muss die Firewall dasselbe Schutzniveau bieten.
- **Proaktive Content-Kontrolle**: Die Firewall sollte auf Wunsch des Nutzers proaktiv potenziell gefährliche Anwendungen blockieren, etwa ActiveX sowie Java-Applets und -Scripts.

## Einsatz von mehreren Firewalls

Seit Veröffentlichung von Service Pack 2 für Windows XP im Dezember 2004 enthalten alle Windows-Versionen eine integrierte Firewall. Sie stellt grundlegende Sicherheitsfunktionen zur Verfügung. Einen umfassenderen Schutz bieten jedoch die Firewalls, die in Security-Softwarepaketen von renommierten Anbietern wie Bitdefender enthalten ist.

Wichtig ist, dass auf einem Rechner nur eine Personal Firewall verwendet werden sollte. Der Parallelbetrieb der Firewall von Windows und eines anderen Anbieters führt zu Fehlfunktionen. Aus diesem Grund deaktivieren Sicherheitssoftware, wie etwa die von Bitdefender, bei der Installation die Windows-Firewall.

Copyright © BitDefender 2012

## Fazit

Ohne Firewall ist ein sicherer Internet-Zugang nicht denkbar. Bei der Wahl entsprechender Produkte sollte der Anwender nicht nur den Funktionsumfang der betreffenden Lösung prüfen, sondern auch, ob sich die Software komfortabel konfigurieren lässt. Am einfachsten ist es, ein Komplettpaket zu verwenden, das einen Viren-, Phishing- und Spyware-Schutz mit einer Firewall kombiniert. Einige Lösungen, wie etwa Bitdefender Total Security 2013, erlauben zusätzlich ein Online-Backup von wichtigen Daten.


(Bild: Bitdefender)

Führende IT-Security-Lösungen, wie etwa Bitdefender Internet Security 2013, sind mit einer integrierten Personal Firewall ausgestattet. Mit ihr lässt sich steuern, welche Netzwerk-Services von außen auf den Rechner zugreifen dürfen und welchen Anwendungen gestattet ist, eine Internet-Verbindung aufzubauen.

Copyright © BitDefender 2012