Business-PC Daily-Newsletter

Was macht eigentlich eine Personal Firewall?

Kaum ein Tag vergeht, an dem nicht eine neue Virenwarnung die Runde macht, ein neues Sicherheitsloch entdeckt oder von verheerenden Angriffswellen aus dem Internet berichtet wird. Kein Wunder, dass sich immer mehr Anwender sorgen, ob nicht auch ihr Rechner Ziel übler Hackerattacken werden kann.

Schutz versprechen hier die so genannten "Personal Firewalls". Das sind spezielle Programme, die, einmal installiert, unerwünschte Zugriffe aus dem Netz zuverlässig abwehren sollen. Rundumsorglose Sicherheit auf Mausklick. Das klingt schön einfach – und ist doch einfach nur zu schön, um wahr zu sein.

So kommuniziert Ihr PC mit dem Internet

Der gesamte Datenverkehr im Internet wird über so genannte Ports abgewickelt. Von denen besitzt ein Internet-PC jede Menge, nämlich genau 65.536. Programme, die via Internet Kontakt zu anderen Computern aufnehmen, senden über einen solchen Port Daten oder warten an einem Port darauf, dass Daten geschickt werden (dann "lauscht" die Software an diesem Port).

Ports, über die weder Daten verschickt noch empfangen werden, sind inaktiv. Einige dieser Ports dienen wohl definierten Aufgaben, andere stehen zur freien Verfügung. So erwartet ein Webserver typischerweise Browser-Anfragen am Port 80. Sie können das ausprobieren, in dem Sie die Portnummer mit einem Doppelpunkt an den Domainnamen hängen. Mit

http://www.torsten-fechner.de:80/

fordern Sie als Client an Port 80 des Servers die vertraute Webseite von Computerwissen an. Mit

http://www.torsten-fechner.de:79/

kontaktieren Sie ebenfalls den Webserver, diesmal allerdings an Port 79 – und erhalten eine Fehlermeldung, weil der Server nur an Port 80 auf HTTP-Anfragen reagiert

Im Prinzip versucht ein Angreifer via Internet bei Ihrem PC nichts anderes: er überprüft, ob an einem Port eventuell eine Software lauscht, über die er in den PC eindringen kann.

Das leisten Personal Firewalls

Und genau hier setzen Personal Firewalls an: Sie kontrollieren den Datenverkehr, der über die verschiedenen Ports läuft. Dazu wird zuerst der gesamte Datenstrom blockiert und anschließend

Stück für Stück frei gegeben. Sobald ein Programm versucht, über einen Port Daten zu schicken oder zu empfangen, wird dies von der Personal Firewall bemerkt und der Anwender informiert.

Der muss dann entscheiden, ob das Programm die gewünschte Aktion ausführen darf oder nicht. Nach der Installation der virtuellen Brandmauer haben Sie also erst einmal alle Hände voll zu tun, um Ihrer Internet-Software – vom E-Mail-Programm über den Chat-Client bis zum Webbrowser – den Zugriff aufs Internet frei zu geben.

Auch beim Gegenverkehr wacht die Personal Firewall über die Rechnerports und blockt Zugriffe von außen dann ab, wenn ein Programm angesprochen wird, das nicht mit dem Internet kommunizieren darf.

Angriffs-Szenario

Wie sieht nun ein möglicher Angriff aus dem Internet aus, vor den die Personal Firewall schützen soll? Da versucht also jemand über einen so genannten Portscan einen "offenen Port" auf Ihrem Rechner zu finden. Eine Personal Firewall meldet hier häufig einen versuchten Angriff, den sie abgewehrt habe.

Eine solche Meldung klingt gut und beruhigend, ist meist aber nur überflüssig: Der Angriff wäre auch ohne Personal Firewall genau so gescheitert, wie der Versuch, den Server auf Port 79 zu erreichen.

Viele der angeblichen Angriffe von außen entpuppen sich am Ende gar als völlig normale Funktionen der Internet-Software, etwa der Versuch, über Port 6346 Kontakt zu Ihrem Rechner aufzunehmen: An diesem Port lauscht normalerweise "Gnutella"-Software und jeder Surfer, der an dieser Tauschbörse teil nimmt, wird von anderen Gnutella-Anwendern über diesen Port kontaktet.

Von hier ab wird's gefährlich

Wirklich gefährlich wird die Sache erst dann, wenn Sie sich – etwa durch das unbedachte Öffnen einer Datei – einen Virus eingefangen haben, der eine Backdoor installiert. Dabei wird ein vom System nicht benutzter Port – und bei über 65.000 gibt es davon eine reichhaltige Auswahl – heimlich geöffnet.

Durch diese Backdoor kann es einem Einbrecher gelingen, Ihren PC via Internet zu kapern. Hier schlägt die große Stunde der Personal Firewall: denn die bemerkt den Eindringling und sperrt ihn umgehend aus, bevor er Schaden anrichten kann. Auch der Versuch von Spyware, Daten von Ihrem PC zu verschicken, kann eine Personal Firewall unterbinden – vorausgesetzt, Sie haben die Spyware als solche erkannt und ihr nicht den Zugriff aufs Internet gestattet.

Eine Personal Firewall bekämpft Symptome – keine Ursachen

In diesen beiden Fällen ist eine Personal Firewall also tatsächlich hilfreich – und beide Male setzt sie nur bei den Symptomen an, nicht bei den Ursachen: Sowohl Backdoor als auch Spyware befinden sich nach wie vor im System und stellen nach wie vor eine Bedrohung dar.

Der einzige echte Schutz gegen eine unerwünschten Seiteneingänge und Schnüffelsoftware besteht darin, sie gar nicht erst zu installieren: Dabei helfen Ihnen besonnenes Verhalten und ein guter Virenscanner – aber keine Personal Firewall.

Die ist auch machtlos, wenn ein Programm, dem Sie den Zugriff aufs Internet erlaubt haben, eine Sicherheitslücke besitzt oder wenn Sie per E-Mail einen Virus geschickt bekommen. Schließlich dürfen diese Programm mit dem Internet kommunizieren – welche Inhalte da durchs Netz wandern, ob Virus oder Mail, kann eine Personal Firewall nicht entscheiden.

Sind diese Programme also schlicht nur unnützer Tand? Das nun nicht gerade, doch ist ihre Schutzfunktion eher bescheiden. So liegt ihr größter Nutzen denn auch woanders: Eine Personal Firewall kann Ihnen ein Gespür dafür vermitteln, wo Sie sind, wenn Sie "im Internet" sind: In einem quicklebendigem Netzwerk, in dem Datenpakete pausenlos hin- und herflitzen und es völlig normal ist, dass alle paar Minuten jemand anklopft. Man muss ihn ja nicht rein lassen.