

Warum Desktop Firewalls gefährlich sind.

Desktop Firewalls sind grundsätzlich nur etwas für sehr paranoide Menschen und wenn sie eingesetzt werden sollten, dann nur von Menschen, die Experten auf dem Gebiet der Netzwerke sind.

Desktop oder auch Personal Firewalls (im folgenden PF oder nur Firewall) sollen einen einzelnen Computer davor schützen „von Hackern angegriffen zu werden“. Dazu blockieren sie zum einen von außen (aus dem Internet) kommende Anfragen und zum anderen verhindern sie, dass Programme auf dem eigenen PC sich ohne Erlaubnis ins Internet oder generell zu anderen Computern verbinden.

Gerade an diesen Stellen lauern aber latente Gefahren.

In Netzwerken (und um ein solches handelt es sich auch beim Internet) werden alle Daten in kleine Pakete verpackt und dann einzeln verschickt. Eine PF untersucht diese Pakete auf schädliche Wirkung und filtert schlechte Pakete aus. Genau hier aber können böswillige Zeitgenossen ansetzen.

Keine Software ist fehlerfrei¹, das schließt explizit auch Firewalls mit ein. Findet ein Hacker einen Fehler in der Software, kann er der Firewall Pakete unterschieben, die genau das Gegenteil von dem bewirken, was sie eigentlich tun soll. Der Hacker kann die Firewall ausschalten, umgehen oder im schlimmsten Fall Kontrolle über die Firewall übernehmen. Da die Firewall auf dem eigenen Rechner läuft, wird sie als vertrauenswürdig eingestuft und hat unbeschränkten Zugriff auf den ganzen Computer. Kontrolliert der Hacker die Firewall, kontrolliert er auch den Computer!

Umgekehrt ist es einer PF auch nicht komplett möglich zu verhindern, dass Schadsoftware, die sich schon auf dem Rechner befindet sich ins Internet verbindet. Häufig hängen sich solche bösen Programme huckepack an solche von denen man als Benutzer „genau weiß“, dass sie ungefährlich sind, wie den Internet Browser oder das Emailprogramm. Die Firewall „sieht“ nur, dass sich ein vertrautes Programm verbinden möchte, ist aber nicht in der Lage zu entscheiden, ob die transportierten Pakete gut oder böse sind.

Und wer weiß als Benutzer schon ganz genau, was sich dahinterverbirgt, wenn die Firewall meldet, dass sich zum Beispiel das Programm „svchost.exe“ ins Internet verbinden möchte.

Desktopfirewalls erzeugen ein trügerisches Gefühl von Sicherheit. Sie bewahren einen Computer nicht vor Fehlern eines Anwenders, der einen verseuchten Emailanhang öffnet oder im Internet auf einen Link klickt, der einen Trojaner installiert. Sie können in versierten Händen und nach sorgfältiger Konfiguration eine Hilfe sein einen Computer zu schützen, können aber auch leicht das Gegenteil bewirken, wenn sich der Anwender

¹ s. z.B. <http://www.heise.de/security/news/meldung/68725> oder <http://www.heise.de/security/news/meldung/92599>

hinter seiner Firewall sicher fühlt und keinen Gedanken mehr daran verschwendet, wie gefährlich das Internet sein kann.