

## Firewalls und Hackers

### Zusammenfassung

Um PCs gegen Angriffe von aussen zu schützen, benützt man eine „Firewall“ (=Brandmauer). Dabei unterscheidet man zwischen „Hardware Firewall“ und „Software Firewall“. Beide sollten aktiv sein. Diese Merkblatt zeigt, wie man herausfindet, ob sie aktiv sind.

Bitte die folgenden Punkte beachten:

- „Keine“ Software Firewall ist schlecht.
- „Eine“ Software Firewall ist gut.
- Mehr als eine Software Firewall ist schlecht.
- **Die meisten Hacker-Angriffe gelingen, weil der PC-Besitzer den Angreifer unbewusst an den Firewalls vorbeischiebst und in sein System lässt.**

Beispiel: Er klickt etwas auf einer unbekanntenen Seite, das ihm einen Preis verspricht.

### Hardware Firewall

Ein Router ist eine Hardware Firewall. Manche Modems haben einen Router bereits eingebaut, ohne dass der Besitzer es weiss. Ob man einen Router installiert hat, sieht man an seiner internen IP-Adresse. Interne Adressen, die so anfangen, sind gut:

- 192.168 . . .
- 10.0 . . .

Alle ändern internen Adressen deuten an, dass man keinen Router hat. In diesem Fall muss man einen installieren. Beispiel:

- 45.23.127.12

Seine interne IP Adresse findet man auf einem PC so heraus:

1. Die Windows-Taste + R drücken.
2. Diese Befehle eingeben:  
mode con lines=50 {Enter}  
ipconfig.exe {Enter}
3. Kontrollieren, was es auf der Zeile „IPv4 Address“ heisst. Sie könnte so lauten:  
IPv4-Adresse . . . . . : **192.168**.11.92

### Software Firewall

Ob die Windows Firewall aktiv oder inaktiv ist, kontrolliert man so:

1. Die Windows-Taste + R drücken.
2. Diesen Befehl eingeben:  
control.exe {Enter}
3. Oben links „Kleine Symbole“ klicken.
4. Unten „Windows Firewall“ klicken.
5. Auf der rechten Seite „Ein- oder ausschalten“ klicken, falls nötig.