# Desktop/Personal Firewalls (PFW)
## *- und warum man sie nicht braucht*

- eine Firewall ist ein Sicherheits**konzept**, und keine Software, die man einfach installiert.
  *Will man einen Rechner oder ein Netzwerk schützen, benötigt man zuallererst einmal ein Konzept. Daher geht die Sprachregelung meistens auch eher dahin, daß man, wenn man von "der Firewall" spricht, zunächst einmal dieses Konzept meint. Dieses beinhaltet u.a., das man sich fragt, was man vor welcher Art von Angriff schützen möchte.*
- eine Firewall, die auf dem System läuft, welches geschützt werden soll, ist oft **sinnfrei**, da sie es ja gerade verhindern muß, daß schädigende Datenpakete zum zu schützenden System vordringen können.
  *So sind evtl. bereits anfällige Komponenten, welche hätten geschützt werden sollen, durchlaufen worden, bevor die Firewall überhaupt eingreifen konnte. Gleichzeitig wird die Komplexität des zu schützenden Systems erhöht.*
- jedes zusätzliche Programm auf einem System erhöht die Anfälligkeit, da Programme und damit auch PFW's **Fehler und Sicherheitslücken** enthalten, die sich in ihrer Anzahl summieren können.
  *Die Komplexität des zu schützenden Systems wird erhöht. Mehr Komplexität heißt aber zwangsläufig mehr Fehlermöglichkeiten und damit weniger Sicherheit.*
- sie täuscht dem Benutzer eine **falsche Sicherheit** vor, da er denkt, er wäre jetzt rundum geschützt. In Wahrheit wird er dadurch allzuoft nur nachlässiger - dies wird häufig auch als "Risikokompensation" bezeichnet.
  *Viele werden schon einmal Benutzer gesehen haben, die ohne eine Sekunde des Nachdenkens ein EMail-Attachment geöffnet hatten - und wenn man nachfragt, ob sie keine Bedenken haben, da könnte ein Virus drin sein, kommt fast immer "Wieso, ich hab doch ein Antivirus-Tool!".*
- Personal/Desktop-Firewalls können problemlos **umgangen und ausgeschaltet** werden, ohne das der Benutzer davon etwas bemerkt.
  *Vor allem die Regelanpassung zur Laufzeit ist als kritisch anzusehen, da Dialogboxen von Würmern o.ä. schneller 'weggeklickt' werden können, als das sie der Benutzer je zu Gesicht bekommt. Und Regeln, die der Anwender selbst definieren kann, sofern er diese auch versteht, kann auch ein Wurm verändern, da PFW's meist mit den Rechten des angemeldeten Benutzers ausgeführt werden.*

Einige Beispiele, auf die man besser verzichten sollte: *Norton Internet Security und Norton Personal Firewall, BlackIce (Defender), ZoneAlarm, Sygate Personal Firewall, Lockdown2000, Outpost u.a....*
(siehe auch http://www.udel.de/faq/ und http://copton.net/vortraege/pfw/index.html)

*Überreicht durch: Entropia e.V., Steinstraße 23, 76133 Karlsruhe, http://www.entropia.de*
*Urheber: www.ntsvcfg.de, Torsten Mann, Albert-Schweitzer-Str. 6, 01187 Dresden*