
Die perfekte Personal Firewall, gibt es sie?



Fraunhofer Institut
Naturwissenschaftlich-
Technische Trendanalysen

Wilfried Gericke

Dr.Phil(USA) Dipl.-Math

IT-Sicherheitsbeauftragter

Die perfekte Personal Firewall, gibt es sie ?

Inhalt:

Motivation

Grundlagen Firewall

Grundlagen Personal Firewall

Beispiele von Personal Firewalls

Benutzung von Personal Firewalls

Fazit

Seite 2

Vortrag 1M03 DECUS Symposium 2006

Fraunhofer 
Institut
Naturwissenschaftlich-
Technische Trendanalysen

Die perfekte Personal Firewall, gibt es sie ?

Motivation

IT-Sicherheit geht jeden etwas an !

Warum:

Jeder kann die IT nutzen, insbesondere das Internet.

Der Endnutzer benötigt kaum noch Fachwissen zum Benutzen des Internet.

Die Nutzung des Internet ist fast obligatorisch; auch im privaten Umfeld.

Aber nicht alle Menschen haben gute Absichten.

Seite 3

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Motivation

Der Internet-User muss sich schützen bzw. soll geschützt werden

Sicherheit ist nicht kostenlos

- gesetzliche Auflagen
- betriebswirtschaftliche Kosten/Nutzen-Analyse

Sicherheitsmodelle

- keine Sicherheit
- Sicherheit durch Täuschung
- Rechnerzentrierte Sicherheit
- Netzwerkzentrierte Sicherheit

Seite 4

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Motivation

Netzwerkzentrierte Sicherheit

Einsatz von Firewalls

Standard Netzwerkfirewall (Absicherung eines Rechnernetzwerk)

Personal Firewall (Absicherung eines Rechners)

Der Einsatz einer Netzwerk-Firewall reicht nicht aus !

Welche Personal Firewall sollte man einsetzen ?

Seite 5

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Firewall

Eine Firewall dient dazu, ein internes Netzwerk mit einem öffentlichen Netzwerk zu verbinden, von dem man annehmen muss, dass es potentielle Angreifer beherbergt. Dabei sollen den internen Nutzern die Vorteile des Internets zugänglich gemacht werden, ohne dabei Unbefugten Zugriff auf interne Daten zu ermöglichen.

Eine Firewall besteht aus einer oder mehreren Hard- und Softwarekomponenten, die zwei Netzwerke koppeln und sicherstellen, dass jeglicher Verkehr zwischen den beiden Netzen durch die Firewall kontrolliert geleitet wird.

Was leistet eine Firewall ?

- Fokus für Sicherheitsentscheidungen
- Zentraler Verbindungsknoten
- Begrenzung der Angriffsfläche für externe Angreifer

Seite 6

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Firewall

Eine „Netzwerk-Firewall“ leistet keinen Schutz vor:

- Angriffe durch Insider
- Umgehung durch weitere Datenleitungen
- Viren, Trojaner etc.
- unbekannte Gefahren

Firewallklassen:

- Paketfilter**
- Verbindungsgateway**
- Applikationsfilter**

Seite 7

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Firewall

Paketfilter

Access Control List – Technik auf

Netzwerk-Layer (OSI-Schicht 3)

IP-Layer des TCP/IP-Modells (OSI-Schicht 5,6,7)

Jedes Paket wird vor der Weiterleitung mit einer Anzahl von Regeln (Sec-Policy) verglichen

Tool um

- ungebetene Dienste zu verbieten
- Zugriffsrechte auf bestimmte Rechner zu definieren

Schwachstelle

- Missbräuchliche Nutzung von Ports kann nicht erkannt werden
- Es können nur IP-Adressen und Ports gesperrt werden
- Es können Angriffe auf bestimmte Ports unternommen werden

Seite 8

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Firewall

Verbindungsgateway

Transport-Layer (OSI-Schicht 4)
Proxy-Server (engl. Stellvertreter)
NAT (Network Address Translation)

Schwachstelle

Kontrolle der Pakete findet normalerweise nicht statt

Seite 9

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Firewall

Applikationsfilter

Application Layer (OSI-Schicht 7)
Liest den Inhalt von Paketen
Versteht Protokolle, kann Befehle in Anwendungsprotokollen filtern.

Schwachstelle:

- Sicherheitslöcher in Protokollen können nicht verhindert werden

Seite 10

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Seite 11

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Personal Firewall (auch Desktop Firewall genannt)

eine Firewall, die kein Rechnernetz sondern einen Rechner schützt, auf dem die Firewall installiert ist

- Paketfilter,

kontrolliert den Datenfluss für den ein- und ausgehenden Verkehr nach den Regeln des Nutzers

- Application-Filter,

kontrolliert Programme, die mit dem Internet Verbindung aufnehmen

z.B.. MS-Office, Corel Draw, Virens Scanner, ...

nach Vorgabe des Nutzers

Seite 12

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Personal Firewall

Sie kann die individuellen Schutzbedürfnisse des Nutzers dedizierter berücksichtigen.

Seite 13

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Personal Firewall

Aufgaben einer Personal Firewall

- IP-Adressfilter
- Portfilter
- Kontrolle der Verbindungen
 - von Außen: Angriffe, Portscans, etc.
 - von Innen: lokale Applikationen eröffnen Verbindungen nach Außen (Spyware, Trojaner, „Homephone“)
- Warnen vor unbekanntem Verbindungsaufbau

Seite 14

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Grundlagen Personal Firewall

Eine personal Firewall ersetzt keine „Netzwerk-Firewall“

- sie ist abschaltbar
- kann umgangen werden

weitere Nachteile einer Personal Firewall

- Nutzer könnte Admin-Rechte haben
- eine gute Konfiguration einer Personal Firewall überfordert den normalen Nutzer
- eine Personal Firewall suggeriert oft mehr Sicherheit als sie bietet

Seite 15

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenlos :

Internet Connection Firewall (ICF) in WindowsXP eingebaut

Zone Alarm

Kerio Personal Firewall

Sygate Personal Firewall

Outpost

Security Suites: viele

Seite 16

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenfreie und deutschsprachige Version von Microsoft

Internet Connection Firewall (ICF) in WindowsXP

Diese WindowsXP-Firewall bietet wirklich nur Schutz vor Angriffen von außen.

Besser als keine Firewall, jedoch nicht ausreichend !

Seite 17

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenfreie und deutschsprachige Version Sygate Personal Firewall 5.5

- System zur Erkennung von Angriffen (Intruder Detection System)
- Protokollschutz auf allen 4 Ebenen des Netzwerk-Protokolls TCP/IP
- Schutz gegen wiederholte Angriffsversuche (Active Response)
- Erkennung von verfälschten Quell IP-u. MAC-Adressen (Anti-IP & Anti-MAC Spoofing)
- Schutz vor Veränderungen an Programmen u. DLL-Dateien durch Trojaner od. Viren (Application DLL Authentication)
- Schutz vor Prozessdeaktivierung (Firewall Termination Prevention)
- Sicherheit auf mehreren Ebenen (Multilayer-Firewall)
- Angriffsrückverfolgung/IP-Zielinformationen (Backtrace/WHOIS)
- TCP/IP-, UDP- und ICMP-IP-Schutz
- Automatische Einrichtung und selbständiger Schutz nach der Installation
- Umfangreiche Statistikfunktionen

**Lizenz: Freeware
Sprache: Deutsch**

Seite 18

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenfreie und deutschsprachige Version Sygate Personal Firewall 5.5

Software

- Windows XP Home Edition und Professional (alle Service Packs)
- Windows 2000 Professional (alle Service Packs)
- Windows NT 4.0 Workstation mit Service Pack 5 oder höher
- Windows 95/98 (alle Service Packs)
- Windows Me (alle Service Packs)
- Microsoft Internet Explorer ab Version 4.0

Zugriffsrechte

- Um die Firewall zu installieren und zu konfigurieren, benötigt man auf dem System lokale Administratorrechte.

Seite 19

Vortrag 1M03 DECUS Symposium 2006



Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenfreie und englischsprachige Version von ZoneAlarm 6.1

- System zur Erkennung von Angriffen (Intruder Detection System)
- Protokollschutz für TCP/IP
- Schutz gegen wiederholte Angriffsversuche (Active Response)
- Schutz vor Veränderungen an Programmen u. DLL-Dateien durch Trojaner od. Viren (Application DLL Authentication)
- Schutz vor Prozessdeaktivierung (Firewall Termination Prevention)
- Sicherheit auf mehreren Ebenen (Multilayer-Firewall)
- TCP/IP-, UDP- und ICMP-IP-Schutz
- Automatische Einrichtung und selbständiger Schutz nach der Installation
- Umfangreiche Statistikfunktionen

Lizenz: Freeware
Sprache: Englisch

Seite 20

Vortrag 1M03 DECUS Symposium 2006



Die perfekte Personal Firewall, gibt es sie ?

Beispiele von Personal Firewalls für Windows-Rechner:

kostenfreie und englischsprachige Version von ZoneAlarm 6.1

Software

- Windows XP Home Edition und Professional (alle Service Packs)
- Windows 2000 Professional (alle Service Packs)
- Windows NT 4.0 Workstation mit Service Pack 5 oder höher
- Windows 95/98 (alle Service Packs)
- Windows Me (alle Service Packs)
- Microsoft Internet Explorer ab Version 4.0

Zugriffsrechte

- Um die Firewall zu installieren und zu konfigurieren, benötigt man auf dem System lokale Administratorrechte.

Seite 21

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Benutzung von Personal Firewalls

Die Installation einer Personal Firewall ist mit Hilfe von Installationswizards für den normalen Nutzer machbar !

Paket-Filter-Funktionalität:

- in einem Unternehmungsnetz wird diese Funktionalität von der „Netz-Firewall“ abgedeckt
- bei einem mobilen Arbeitsplatz muss diese Funktionalität durch die Personal Firewall abgedeckt werden

Seite 22

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Benutzung von Personal Firewalls

Port- und IP-Adressen-Filter in Windows

Eigenschaften von Netzwerk-Verbindungen

Eigenschaften von Internet-Protokoll

erweitert

Optionen

Eigenschaften

Seite 23

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Benutzung von Personal Firewalls

Port- und IP-Adressen-Filter

Rechner kommunizieren über das IP-Protokoll (TCP und UDP)

Beide verwenden Port-Adressen, um die Daten an den betreffenden Dienst der Anwendungsebene zu senden.

Um Konflikte zu vermeiden, müssen verschiedene Services auch verschiedene Ports verwenden

Ports < 1024 sind nur privilegiert erreichbar (Admin)

Den Ports sind bestimmte Dienste zugeordnet

Seite 24

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Benutzung von Personal Firewalls

Übersicht Ports, IP-Protokolle und Anwendungen

Seite 25

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Benutzung von Personal Firewalls

Application-Filter

Grundlegende Programme benötigen auf jeden Fall Zugriff auf das Internet

SVCHOST.exe (Generic Host Process for Win 32 Services)

Browser

Email-Programm

...

Seite 26

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Hilfstoos

**pcwProcview zeigt alle aktiven Programme an und sucht nach den Namen bei Google
(kostenlos)**

**TCP-View listet alle TCP- und UDP-Verbindungen auf
(kostenlos)**

netstat.exe -b (standard Windows-Tool)

Seite 27

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Flankierende Schutzmaßnahmen:

regelmäßige Updates durchführen von

- Windows (Security-Updates)
- Virenschanner
- Antispy- und Anti-Adware-Tools
- Personal Firewall Software

nicht mit Admin-Rechten online gehen, sondern mit Nutzer-Konto mit beschränkten Nutzerrechten

Seite 28

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Fazit

Es ist fahrlässig, einen Rechner bzw. ein Rechnernetz nicht durch eine Firewall abzusichern.

Bald wird auch die Justiz den Einsatz von Firewalls fordern, wie es bei Virenscannern schon der Fall ist (im kommerziellen Bereich).

Die perfekte Personal Firewall gibt es nicht !

Sie ist nur ein Teil eines Sicherheitskonzepts und deshalb ist die Auswahl des Produktes von untergeordneter Bedeutung.

Seite 29

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Fazit:

Eine Personal Firewall sollte mit der Netz-Firewall abgestimmt sein, um bei Bedarf die individuellen Bedürfnisse der Nutzer besser zu berücksichtigen.

**Vergleichtest Personal Firewall:
PC-Welt 9/2005**

**Ergebnis: Norton Personal Firewall 2005
ZoneAlarm Pro 5.1
Sygate Personal Firewall Pro 5.5**

Seite 30

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Fazit:

Man sollte Personal-Firewall-Produkte einsetzen,

- von denen es auch eine kostenlose Version gibt, damit die Nutzer diese privat einsetzen können und somit mit den Funktionen vertraut sind
- sie sollten deutschsprachige Versionen haben, um die Akzeptanz beim Anwender für den privaten Bereich zu erhöhen
- die professionelle Version sollte zentral konfiguriert und gepflegt werden können

meine Empfehlung : Sygate Personal Firewall

Seite 31

Vortrag 1M03 DECUS Symposium 2006

Die perfekte Personal Firewall, gibt es sie ?

Fragen ?

Seite 32

Vortrag 1M03 DECUS Symposium 2006