

Netzwerk Elektronischer Geschäftsverkehr

MECK  
Mainfränkisches Electronic  
Commerce Kompetenzzentrum  
meck-online.de

Stuttgart, 01.07.2004

## Firewalls und Sicherheitssysteme für kleine und mittlere Unternehmen

Andreas Gabriel, MECK

Lehrstuhl Prof. Thome

gefördert durch das  
Bundesministerium  
für Wirtschaft und Arbeit

Netzwerk Elektronischer Geschäftsverkehr

MECK  
Mainfränkisches Electronic  
Commerce Kompetenzzentrum  
meck-online.de

© Dipl.-Kfm. A. Gabriel

- MECK ist ein Projekt!
- „gegründet“ 1998
- Projektträger ist die  
IHK Würzburg-Schweinfurt
- Projektpartner

IHK  
Würzburg-Schweinfurt  
Mainfranken

Lehrstuhl Prof. Thome

HWK

<http://www.meck-online.de>

2

## Agenda

© Dipl.-Kfm. A. Gabriel

1. Firewall – Was ist das?
2. Personal Firewalls
  1. Einsatz
  2. Konfiguration
  3. Schwachstellen
3. IT-Sicherheit – Mehr als nur Firewall und Virens Scanner

3

## Firewall – Was ist das?

© Dipl.-Kfm. A. Gabriel



ACCESS  
TO  
HEAVEN  
DENIED

Quelle: [www.viewz.com/cartoon/ cartoon2.shtml](http://www.viewz.com/cartoon/cartoon2.shtml)

4



# Firewall – das Bollwerk vor Ihrem Netzwerk

© Dipl.-Kfm. A. Gabriel

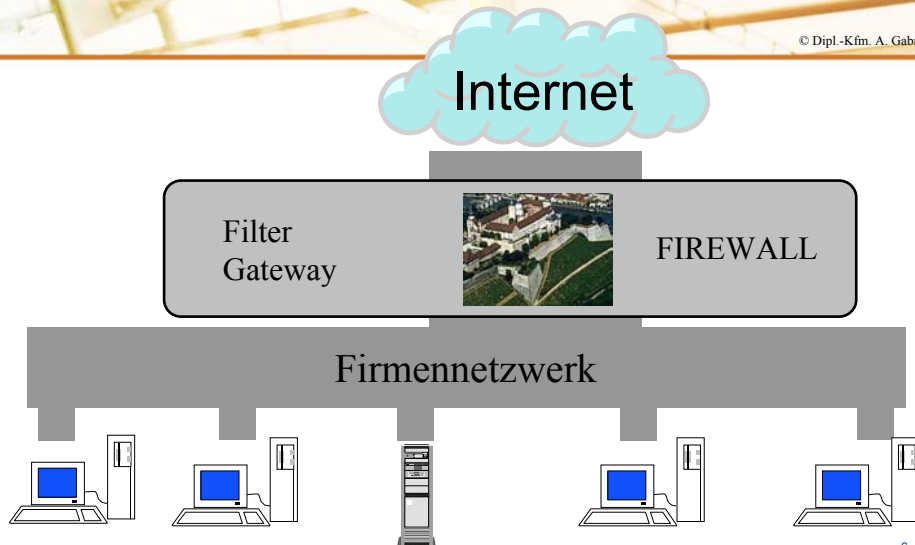


5



# Der Gedanke hinter einer Firewall

© Dipl.-Kfm. A. Gabriel



6

## Firewall – Anforderungsanalyse

© Dipl.-Kfm. A. Gabriel

### Zwingend notwendig sind



mobil



immer konsequent  
und wachsam



Furcht einflößend



abschreckend

### Was darf nie passieren?



Pausen



Ablenkung

7

## Personal Firewalls

© Dipl.-Kfm. A. Gabriel

- Auf jedem Client muss eine eigene Firewall installiert werden
- Dezentrale Lösung
- Programmgröße: ca. 3 MB
- Eng mit dem Betriebssystem verbunden
- Keine umfassende Sicherheit garantiert!

8

## HILFE – Mein Rechner wird angegriffen!

© Dipl.-Kfm. A. Gabriel



9

## Nicht nur für kleine Unternehmen → Personal Firewall

© Dipl.-Kfm. A. Gabriel

- **ZoneAlarm**  
<http://www.zonelabs.com/store/content/home.jsp>
- **Norton Personal Firewall**  
<http://www.symantec.com/sabu/nis/npf>
- **McAfee Personal Firewall**  
<http://www.mcafee.com>
- **Outpost Firewall Pro**  
<http://www.agnitum.com/products/outpost>
- **Tiny Personal Firewall**  
<http://www.tinysoftware.com>
- **Sygate Personal Firewall**  
<http://www.sygate.com>

und  
viele

mehr ...

10

Netzwerk Elektronischer Geschäftsverkehr

M E G K  
Mehrfachliche Funktionen,  
Zusammenhangsgeschichte

## Beispiele „Personal Firewalls“

© Dipl.-Kfm. A. Gabriel

Produkt	Agnitum Outpost	McAfee Firewall	Norman Personal Firewall	Norton Personal Firewall	Sygate Personal Firewall	Tiny Personal Firewall	ZoneAlarm
Version	1.0.1817	4.0	1.20	2003	5.0	4.0	3.1
Installationsgröße (in MB)	3	11	5	15	10	5	10
Preis (circa)	Kostenlos*	34,95 €	39,90 €	49,95 €	Kostenlos*	39,- €	Kostenlos*
<b>Schutz vor Angriffen</b>							
Erkennung von Internet Attacken	++++	+++	+	+++	++++	++++	++++
Darstellung von Netzwerkaktivitäten	++++	+++	++	+++	++++	++++	++++
Verhalten bei Attacken	++++	++++	++	+++	++++	+++	++++
<b>Funktionsumfang</b>							
Schutz vor E-Mail Anhängen	+	-	-	-	-	+	+
Sandbox-Funktion	-	-	-	-	-	+	-
Filter für Pop-Ups und Werbebanner	+	-	+	+	-	-	-
Schutz vor ActiveX	+	-	+	+	-	-	-
Schutz vor Cookies	+	-	+	+	+	-	-
Funktion zur Rückverfolgung	-	+	-	+	+	-	-
<b>Benutzerfreundlichkeit</b>							
Automatische Internet-Programme-Erkennung	-	+	+	+	-	-	-
Vordefinierte Sicherheitsstufen	-	-	-	+	-	-	+
Automatisches Update	+	+	-	+	-	-	+
Benutzerfreundlichkeit des Menüs	++++	+++	+++	++++	++++	++++	++++
<b>Gesamt-Wertung</b>	<b>89%</b>	<b>78%</b>	<b>73%</b>	<b>82%</b>	<b>89%</b>	<b>85%</b>	<b>80%</b>

**Legende:** ein "+" Zeichen bedeutet, das ein Kriterium vorhanden ist. Je mehr "+" Zeichen, desto besser ist das entsprechende Feature gelöst.  
ein "-" Zeichen bedeutet, das der Firewall die entsprechende Funktion fehlt.

\* = Auch in einer erweiterten und kostenpflichtigen Pro-Version erhältlich

Quelle: <http://www.freenet.de>

11

Netzwerk Elektronischer Geschäftsverkehr

M E G K  
Mehrfachliche Funktionen,  
Zusammenhangsgeschichte

## Was ist eigentlich TCP / IP?

© Dipl.-Kfm. A. Gabriel

IP 1 2 3 4 5 6 7 8 Internet Protocol

Internet

TCP  
Transport Control Protocol  
1976 vom US Department of Defence eingeführt

Alternative: UDP  
User Datagramm Protokoll

12



# Beispielkonfiguration anhand der Protokolle

- Beschreibung
- Für wen gilt diese Regel?
- In welche Richtung?
- Für welche (Web-) Adressen gilt diese Regel?
- Zu welchem Zeitpunkt ist diese Regel gültig?
- Erlaubnis/Verbot?
- Protokollierung



# Beispielkonfiguration anhand der Programme

Programmliste

Erlaubnis

noch nicht definiert

Verbot



# Welche Regeln sind sinnvoll bzw. (zwingend) notwendig?

<input type="checkbox"/>	TCP/IP-Befehl Ping	5.00.2134.1	Local: ✓ . . . . ?	Internet: ✗ . . . ✗ .	<input type="checkbox"/>
<input type="checkbox"/>	TCP/IP-Traceroutebefehl	5.00.2134.1	Local: ✓ . . . . ?	Internet: ✗ . . . ✗ .	<input type="checkbox"/>
<input type="checkbox"/>	Windows Explorer	5.00.3502.5321	Local: . . ? . . ?	Internet: . . ? . . ?	<input type="checkbox"/>
<input type="checkbox"/>	Windows Media Player	6.4.09.1121	Local: . . ? . . ?	Internet: . . ? . . ?	<input type="checkbox"/>

- Was ist der „TCP/IP-Traceroutebefehl“?
- Was ist der „TCP/IP-Befehl Ping“?
- Warum muss der Windows Explorer aufs Netz zugreifen?
- Wie muss ich den Windows Media Player konfigurieren?



# Meldungen / Feedback

**NEW PROGRAM**  
ZoneAlarm Program Alert

Do you want to allow Internet Explorer to access the Internet?

**Technical Information**  
Destination IP: 127.0.0.1:Port 1038  
Filename: IEXPLORE.EXE  
Version: 5.00.2800.1106

**More Information Available**  
This is the program's first attempt to access the Internet. [More Info](#)

Remember this answer the next time I use this program.

Yes No

**PROTECTED**  
ZoneAlarm Firewall Alert

The firewall has blocked Internet access to your computer (ICMP Echo Request (Ping)) from 212.187.126.80.

Time: 06.11.2002 14:38:52

[More Info](#)

1st of 3 alerts

Don't show this dialog again

OK

**PROTECTED**  
ZoneAlarm Firewall Alert

The firewall has blocked Internet access to your computer (ICMP Echo Request (Ping)) from 132.187.1.4.

Time: 06.11.2002 14:38:58

[More Info](#)

2nd of 3 alerts

Don't show this dialog again

OK

Tiny Firewall



Zone Alarm



## Was muss man erlauben?

© Dipl.-Kfm. A. Gabriel

- # 22: SSH: Aufbau eines verschlüsselten Datenaustauschs für den externen Zugriff.
- # 80: WWW: Der Web-Server kann auf diesem Port vom Internet erreicht werden und antworten.
- # 3.389: Windows-Remote-Desktop: Hier kann eine verschlüsselte Remote-Desktop-Verbindung hergestellt werden.



**Für den Rest muss gelten: DENY ALL**

17



## Gegen W32.Blaster und W32.Sobig

© Dipl.-Kfm. A. Gabriel

- W32.Blaster  
TCP und UDP („in“ und „out“):  
69, 135, 136, 137, 138, 139, 445, 593, 4.444
- W32.Sobig  
-UDP in: 990 bis 999  
-UDP out: 8.998

18

## Schwächen einer Personal Firewall

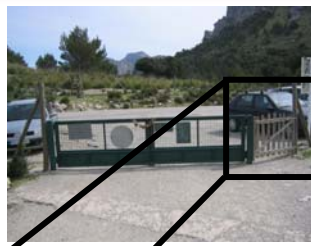
© Dipl.-Kfm. A. Gabriel

- Läuft auf zu schützendem Rechner
- Schützt nur einen PC
- Kann relativ einfach umgangen werden
- Interaktion mit dem Betriebssystem notwendig
- Verbraucht Systemressourcen
- Nutzer hat gesteigertes Sicherheitsgefühl und wird evtl. leichtsinnig
- Warnmeldungen werden zu schnell ignoriert

19

## Auf das Konzept kommt es an!

© Dipl.-Kfm. A. Gabriel



20

## Ermitteln Sie Ihre Anforderungen

© Dipl.-Kfm. A. Gabriel



- Analyse der Bedrohungen
- Bewertung des Bedrohungspotenzials
- Ausrichtung der Sicherheitsstrategie
- Ergreifung geeigneter Maßnahmen
- Kontrolle der gewählten Maßnahmen



21

## Online-Quellen

© Dipl.-Kfm. A. Gabriel

- <http://www.ec-sicherheit.de>
- <http://www.bsi-fuer-buerger.de>
- <http://www.symantec.de>
- <http://www.kaspersky.com>
- <http://www.ccc.org>
- <http://www.astaro.com>
- <http://www.sicherheit-im-internet.de>

22



## Viren, Würmer & Trojaner

© Dipl.-Kfm. A. Gabriel

# Vielen Dank für Ihre Aufmerksamkeit!

Andreas Gabriel

[gabriel@meck-online.de](mailto:gabriel@meck-online.de)



Lehrstuhl Prof. Thome

<http://www.wiinf.uni-wuerzburg.de>



<http://www.meck-online.de>