



# Firewall-Schutz in Kleinunternehmen

Andreas Gabriel, MECK



gefördert durch das

Bundesministerium  
für Wirtschaft und Arbeit



## Firewall: Die Festung vor dem eigenen Netzwerk

© Dipl.-Kfm. A. Gabriel





## Agenda

© Dipl.-Kfm. A. Gabriel

1. Kurze Einführung
2. Darstellung verschiedener Firewall-Konfigurationen
3. Einsatz von Firewalls bei KMU
4. Personal Firewalls – Konfiguration
5. Personal Firewalls – Probleme
6. ROSI

3



## Istsituation: Es vergeht keine Woche ohne Schreckensmeldung

© Dipl.-Kfm. A. Gabriel

**Trojaner nutzt offenes Sicherheitsleck im Internet Explorer**  
02.10.2003

**Trojaner leitet Browser auf falsche Seiten**  
02.10.2003

**Wurm legt Visa-System des US-Außenministeriums lahm**  
24.09.2003

**Wurm legt Schweizerische Post lahm**  
08.10.2003

**Passwort-Klau durch Lücke im Internet Explorer**  
25.09.2003

**RPC-Dienst immer noch offen – Microsoft bessert nach**  
11.09.2003

**Schwächen in Outlooks Web Access**  
09.07.2003

Quellen:

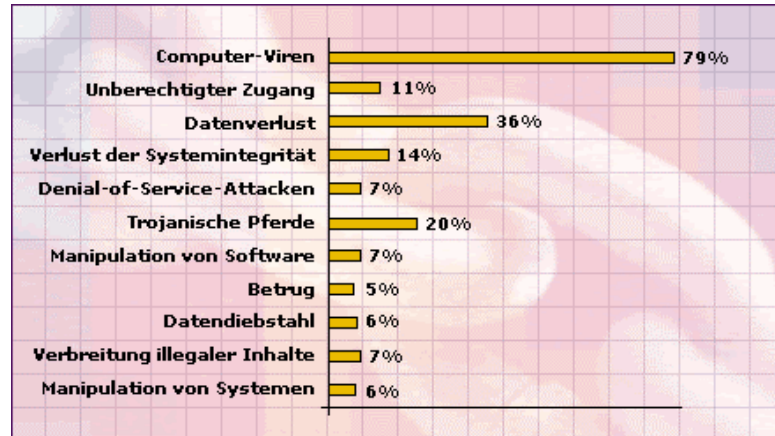


4



## Mit welchen Sicherheitsproblemen wurden Ihr Unternehmen in den letzten 18 Monaten konfrontiert?

© Dipl.-Kfm. A. Gabriel



Quelle: <http://silicon.de>

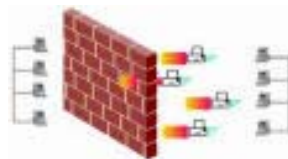
5



## Einsatz einer Firewall

© Dipl.-Kfm. A. Gabriel

- Sobald Sie mit Ihrem Rechner online sind, sind Sie ein Teil eines weltweiten Netzwerkes.
- Dadurch ist Ihr Rechner von außen erreichbar und kann leicht zum Ziel für Angriffe werden.
- Sie können den Zugriff **aus** dem Internet aber auch **in** das Internet steuern!

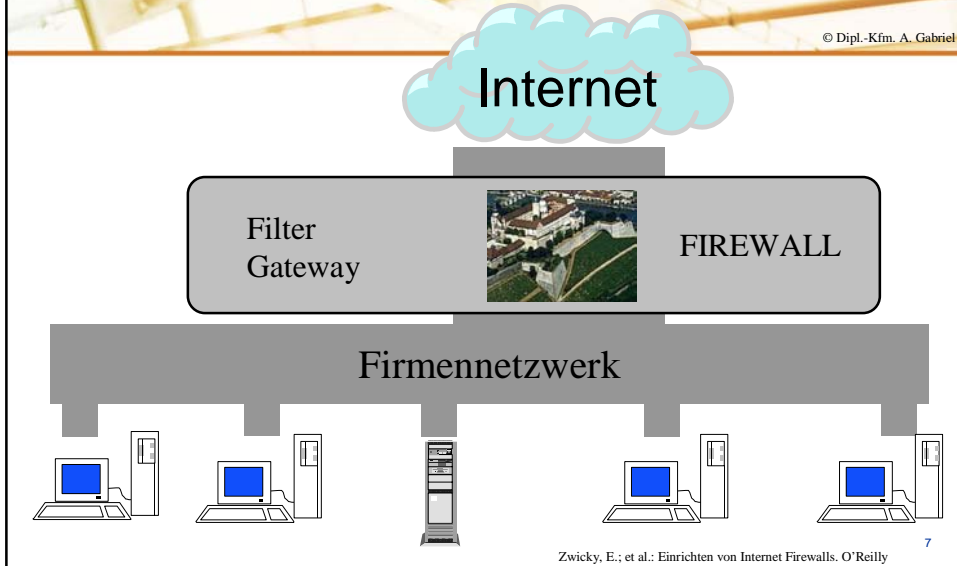


6



## Einrichtung einer Firewall

© Dipl.-Kfm. A. Gabriel

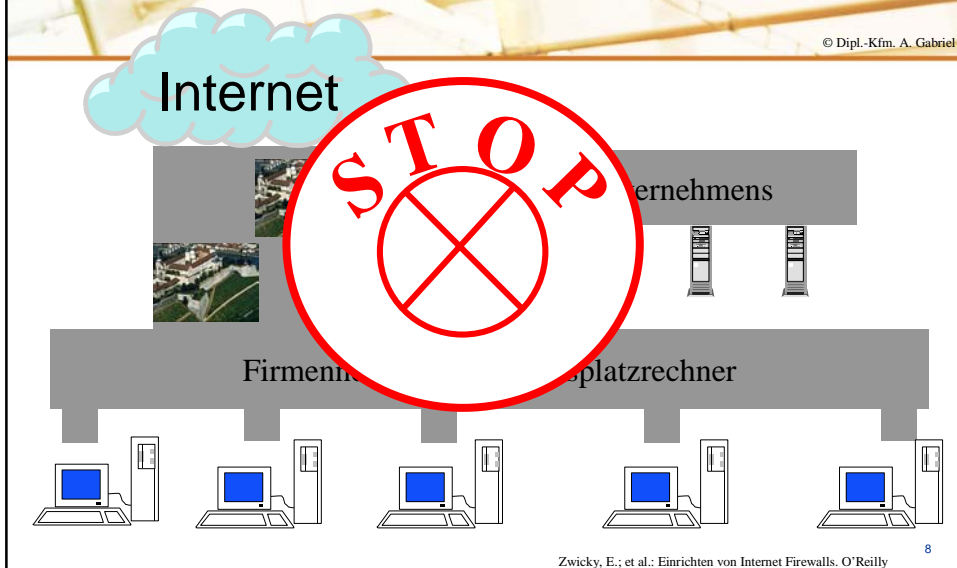


Zwicky, E.; et al.: Einrichten von Internet Firewalls. O'Reilly



## DMZ – demilitarisierte Zone

© Dipl.-Kfm. A. Gabriel



Zwicky, E.; et al.: Einrichten von Internet Firewalls. O'Reilly



## Ausgangssituation in Kleinunternehmen

© Dipl.-Kfm. A. Gabriel

- Die Anzahl der Rechner im Unternehmen ist überschaubar
- Der IT Verantwortliche wird nach der „EDA“ Methode ausgewählt
- Eine Schulung ist quasi nicht existent
- Sensibilisierung zum Thema Sicherheit sehr gering
- Häufige Doppelnutzung des Rechners: privat und beruflich
- Konfiguration des Rechners wird in den seltensten Fällen angepasst

9



## Im Gegensatz dazu ...

© Dipl.-Kfm. A. Gabriel

...wird das Medium Internet bei KMU immer intensiver genutzt!

- eMail-Nutzung
- Eintrag von Marktplätzen
- Online-Banking
- Teilnahme an Online-Ausschreibungen
- Firmeneigene Homepage
- usw.

Plötzlich existieren **neue Probleme:**

Viren, Trojaner, Spam, Dialer, Spyware ...

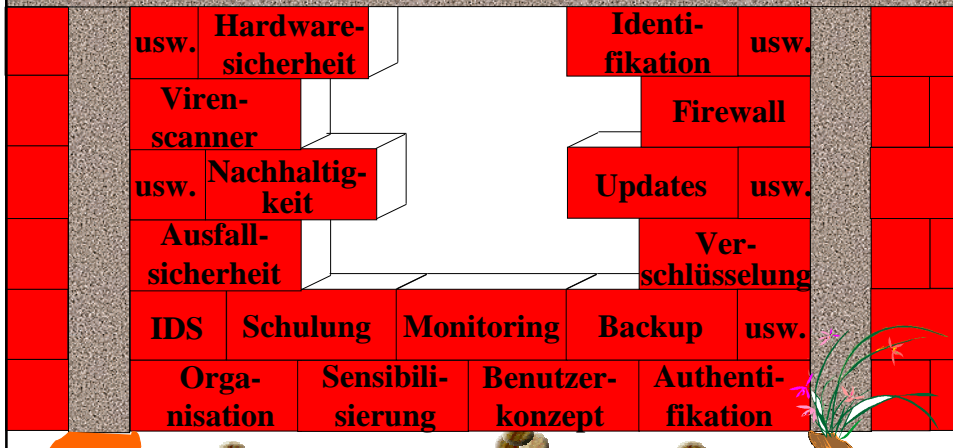
10



## Das schwächste Glied der Kette ...

© Dipl.-Kfm. A. Gabriel

Eine Mauer kann nur schützen, wenn alle Steine halten!



## Lösung 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 ...

12



## Regeldefinition

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  
Protokoll

13



## Einstellungen gegen w32.Blaster

© Dipl.-Kfm. A. Gabriel

- Die Protokolle UDP und TCP sind betroffen
- Die Sperrung muss in beide Richtungen erfolgen
- Folgenden Ports müssen geschlossen werden:
  - 69
  - 135, 136, 137, 138, 139
  - 445
  - 539 und 593
  - 4.444

14

Netzwerk Elektronischer Geschäftsverkehr

MEICK

## 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

15

Netzwerk Elektronischer Geschäftsverkehr

MEICK

## Beispiel: Tiny Firewall gegen w.32

© Dipl.-Kfm. A. Gabriel

Filter rule

Description: w.32

Protocol: TCP and UDP

Direction: Both directions

Local endpoint

Port type: List of ports

List of Ports: 69,135,136,13

Application: Any

Remote endpoint

Address type: Any address

Port type: Any port

Rule valid: Always

Action

Permit

Deny

Log when this rule match

Display alert box when this rule match

OK Cancel

16



## Konfiguration der Personal Firewall

© Dipl.-Kfm. A. Gabriel

ZoneAlarm

UP: [ ] DN: [ ] UP: [ ] DN: [ ] Unlocked

ALERTS LOCK SECURITY PROGRAMS CONFIGURE

| Program                              | Allow connect    | Allow server        | Pass Lock |
|--------------------------------------|------------------|---------------------|-----------|
| \\?C:\WINNT\system32\winlogon.exe    | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| Adobe Acrobat 5.0                    | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| Aladdin StuffIt Expander             | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| Anwendung für Dienste und Controller | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| BSPlayer version 0.8                 | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| BSPlayer version 0.8                 | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| CD-Player                            | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| Handset Manager                      | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |
| HotSync® Manager Application         | Local: ✓ . . . ? | Internet: ✗ . . ✗ . | [ ]       |

Click here to upgrade to ZoneAlarm Pro.

Programmliste

Erlaubnis

noch nicht definiert

Verbot

17



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

© Dipl.-Kfm. A. Gabriel

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

- 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?

18



## Erläuterung des Befehls „Traceroute“

© Dipl.-Kfm. A. Gabriel

Beispiel: C:\>tracert www.yahoo.de

```
Eingabeaufforderung
C:\>tracert www.yahoo.de
Routenverfolgung zu www.euro.yahoo.akadns.net [217.12.3.11] über maximal 30 Abschnitte:

  1  <10 ms    <10 ms    10 ms    wswi34.wiinf.uni-wuerzburg.de [132.187.84.254]
  2  <10 ms    <10 ms    <10 ms    wswi00.atn.uni-wuerzburg.de [132.187.251.253]
  3  <10 ms    <10 ms    <10 ms    wingate.uni-wuerzburg.de [132.187.250.251]
  4  <10 ms    <10 ms    <10 ms    ar-wuerzburg3-ge4-1.g-win.dfn.de [188.1.36.213]
  5  <10 ms    <10 ms    10 ms    cr-erlangen1-po2-1.g-win.dfn.de [188.1.18.218]
  6  100 ms    200 ms    10 ms    cr-stuttgart1-po4-2.g-win.dfn.de [188.1.18.218]
  7  10 ms     10 ms     10 ms    cr-frankfurt1-po8-0.g-win.dfn.de [188.1.18.77]
  8  10 ms     10 ms     10 ms    ir-frankfurt2-po3-0.g-win.dfn.de [188.1.80.42]
  9  10 ms     10 ms     20 ms    ge-3-1-0-8.fra20.ip.tiscali.net [213.200.64.89]
 10  20 ms     30 ms     30 ms    so-3-0-0.lon12.ip.tiscali.net [213.200.81.73]
 11  20 ms     30 ms     30 ms    213.200.77.122
 12  20 ms     30 ms     30 ms    bas14.ukl.yahoo.com [217.12.0.141]
 13  20 ms     30 ms     30 ms    www2.vip.ukl.yahoo.com [217.12.3.11]

Ablaufverfolgung beendet.
C:\>
```

Ergebnis: Yahoo ist unter der IP 217.12.3.11 zu finden<sup>19</sup>



## Erläuterung des Befehls „Ping“

© Dipl.-Kfm. A. Gabriel

Beispiel: C:\>ping 217.12.3.11

```
Eingabeaufforderung
C:\>ping 217.12.3.11
Ping wird ausgeführt für 217.12.3.11 mit 32 Bytes Daten:
Antwort von 217.12.3.11: Bytes=32 Zeit=20ms TTL=243
Antwort von 217.12.3.11: Bytes=32 Zeit=20ms TTL=243
Antwort von 217.12.3.11: Bytes=32 Zeit=20ms TTL=243
Antwort von 217.12.3.11: Bytes=32 Zeit=20ms TTL=243

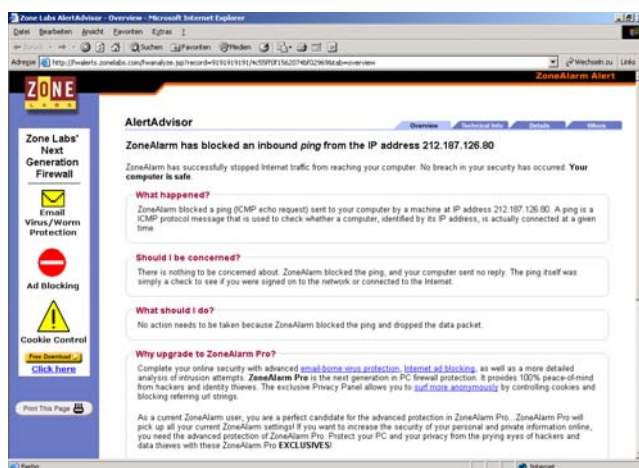
Ping-Statistik für 217.12.3.11:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 20ms, Maximum = 20ms, Mittelwert = 20ms
C:\>_
```





## Angriffsverfolgung

© Dipl.-Kfm. A. Gabriel



23



## 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 weitergeklickt

24



## Return on Security Investment

© Dipl.-Kfm. A. Gabriel

$$\text{ROSI} = \frac{\text{Zusätzliche Umsätze} + \text{Vermiedene Verluste}}{\text{Investitionen in IT-Sicherheit}}$$



Sicherheitsinvestitionen  
sind **keine** Ausgaben  
sondern **Investitionen!**

25



## Firewall-Schutz in Kleinunternehmen

© Dipl.-Kfm. A. Gabriel

# Vielen Dank für Ihre Aufmerksamkeit!

Andreas Gabriel

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



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

26