



**EDV-Beratung Bückemeyer**  
Ebberg 13  
D-58540 Meinerzhagen

fon: +49 [23.58] 90.41.73  
fax: +49 [23.58] 90.42.49  
info@bueckemeyer.com

# Firewall für alle

**Wir sind ein kleines Beratungsunternehmen. In einem schwierigen Marktumfeld die Kunden von dem Wert der Dienstleistungen zu überzeugen ist sicher derzeit nicht ganz einfach. Gespart wird derzeit vor allem recht gerne beim Thema „Netzwerksicherheit“.**  
**Dabei wird die Gefahr häufig unterschätzt, der auch kleine Firmennetzwerke leider ausgeliefert sind.**

Von dem Sinn eines Virenschutzes für alle Emailprogramme im Unternehmen konnten wir einige Kunden schon überzeugen. Das aber ein Rechner, der nur hin und wieder für die Einwahl ins Internet genutzt wird, eine nicht zu unterschätzende Gefahrenquelle darstellt, konnten wir heute wieder beweisen und einem Kunden die Augen öffnen, der dem Thema „Netzwerksicherheit“ sicher künftig eine größere Beachtung schenken wird. Konkret ging es um einen Rechner, der temporär für die Einwahl ins Internet genutzt wird, aber häufig ohne jegliche Firewall stundenlang im Netz hängt. Nach einer Weile kamen die ersten Versuche, den vermeintlichen Windows NT-Rechner auszuspionieren. Dank unserer routinemäßigen Überwachung der Logfiles sahen wir u.a folgendes:

&nbsp;

--

&nbsp;

```
217.229.18.63 - - [23/Jul/2002:12:28:28 +0200] "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 231
```

&nbsp;

```
217.229.18.63 - - [23/Jul/2002:12:28:28 +0200] "GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 231
```

&nbsp;

```
217.229.18.63 - - [23/Jul/2002:12:28:29 +0200] "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 231
```

&nbsp;

```
217.229.18.63 - - [23/Jul/2002:12:28:29 +0200] "GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 404 231
```

&nbsp;

--

&nbsp;

Das Spielchen ging eine Weile weiter, bis der Angreifer - vermutlich ein Skript-Kiddi - nicht mehr weiter kam - bei dem Rechner handelte es sich um ein Linuxsystem. Auf die möglichen Gefahren aufmerksam gemacht, war der Kunde von der Notwendigkeit eines Schutzes für sein Netzwerk überzeugt.

&nbsp;

Insbesondere unsere Gateway-Lösung für kleine und mittlere Unternehmen werden standardmäßig so konfiguriert, dass außer dem Port 22 (für die Fernwartung per ssh) kein Port von außen erreichbar ist.

## **COPYRIGHT**

Alle Beiträge unterliegen, soweit nicht anders gekennzeichnet, dem Copyright von Thomas Bückemeyer. Alle Rechte vorbehalten.