

KONFIGURATION DURCH KONVENTION



WARUM DINGE GANZ EINFACH FUNKTIONIEREN
UND TROTZDEM FLEXIBEL SIND



KONFIGURATION DURCH KONVENTION

- ❖ **Standards**
- ❖ Von Faulheit und Erfolg guter Ideen
- ❖ Vom Erfolg der PHP-Programme
- ❖ Befehle in Shells

STANDARDS

AUTO

MIXER

USB-SCHNITTSTELLE



STANDARDS: AUTO

- ❖ Tür
- ❖ Lenkrad
- ❖ Ich-Bin-Der-Besitzer-Ding
(vulgo: Schlüssel)
- ❖ **Egal welche Marke**
- ❖ **immer gleich**



STANDARDS: MIXER

- ❖ Drei Stufen
- ❖ Haken in Locher stecken
- ❖ In den Teig reinhalten
- ❖ **Egal welche Marke**
- ❖ **immer gleich**



STANDARDS: USB-SCHNITTSTELLE

- ❖ Stecker, gleich
- ❖ Daten
- ❖ Strom laden
- ❖ **Egal welche Marke**
- ❖ **immer gleich**



KONFIGURATION DURCH KONVENTION

- ❖ Standards
- ❖ **Von Faulheit und Erfolg guter Ideen**
- ❖ Vom Erfolg der PHP-Programme
- ❖ Befehle in Shells

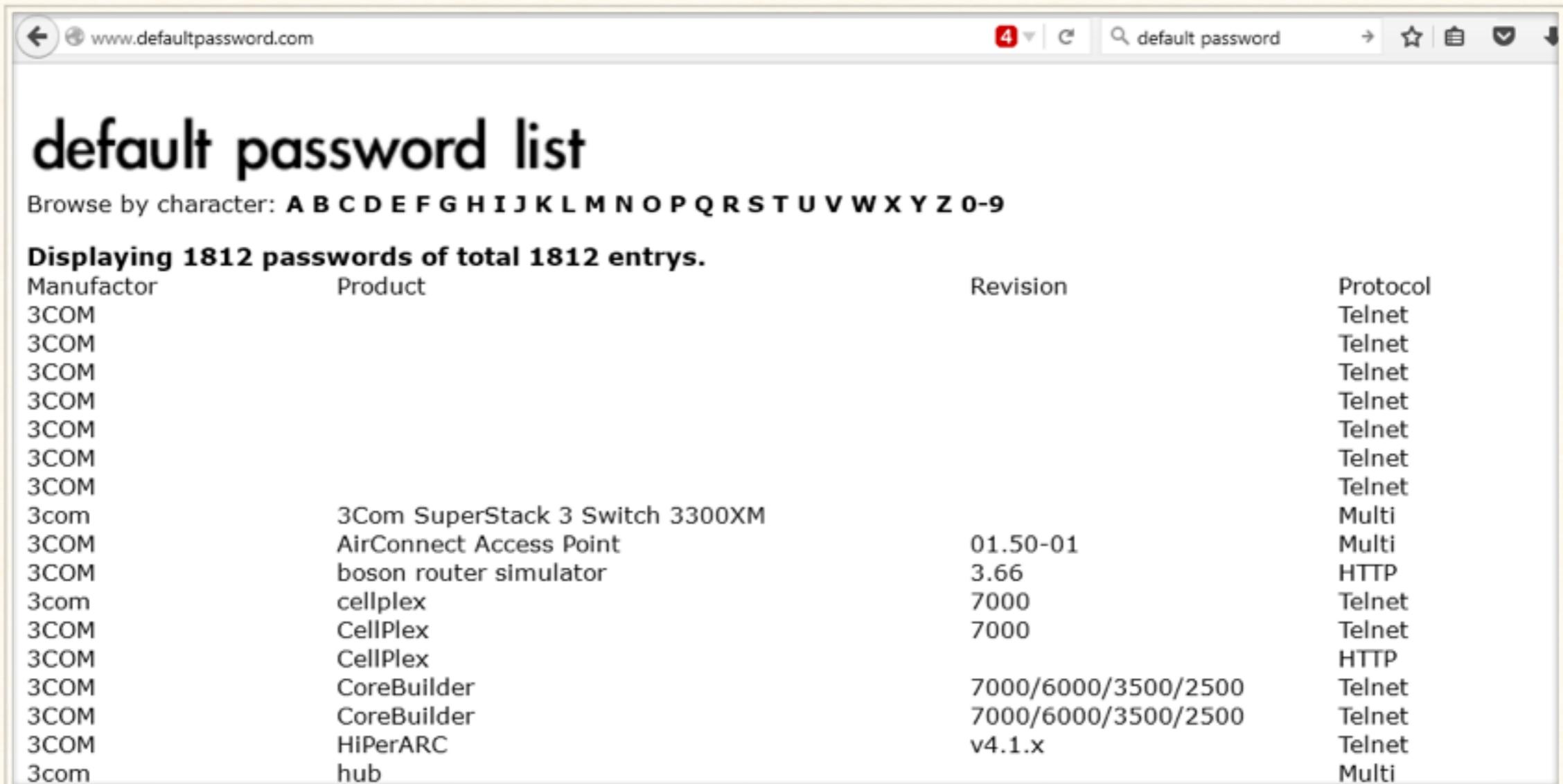
VOR EIN PAAR JAHREN...

- ❖ die meisten Computergeräte hatten ein Standardpasswort
- ❖ 20.000 Router in Vietnam produziert
- ❖ die müssen alle gleich sein



PROBLEM

ANGRIFFE GEGEN DIESE GERÄTE AUS DEM INTERNET



The screenshot shows a web browser window with the address bar displaying 'www.defaultpassword.com'. The page title is 'default password list'. Below the title, there is a navigation bar with the text 'Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9'. The main content area displays a table of 1812 passwords, with the first few rows visible. The table has four columns: 'Manufacturer', 'Product', 'Revision', and 'Protocol'.

Manufacturer	Product	Revision	Protocol
3COM			Telnet
3com	3Com SuperStack 3 Switch 3300XM		Multi
3COM	AirConnect Access Point	01.50-01	Multi
3COM	boson router simulator	3.66	HTTP
3com	cellplex	7000	Telnet
3COM	CellPlex	7000	Telnet
3COM	CellPlex		HTTP
3COM	CoreBuilder	7000/6000/3500/2500	Telnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet
3COM	HiPerARC	v4.1.x	Telnet
3com	hub		Multi

❖ Wie man Geräte aus dem Internet angreift

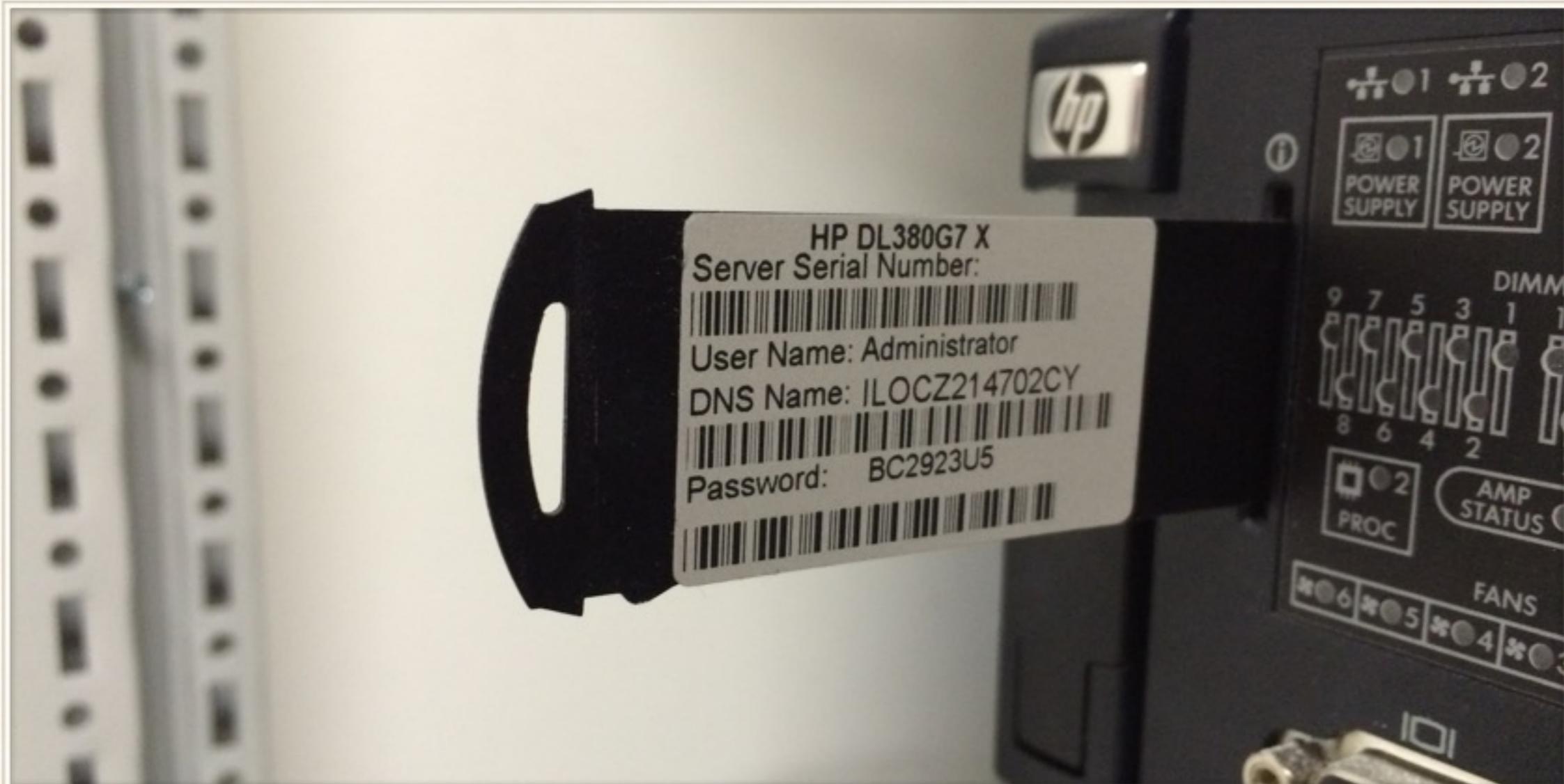
1. Suche einen String aus der Login-Webseite oder Begrüßungsseite des Geräts in Google
2. Klicke auf den ersten Link
3. Probiere das Standardpasswort

❖ Betroffene Geräte

1. Kopierer
2. Drucker
3. Faxgeräte
4. DSL-Router
5. Standardsoftware wie phpmyadmin

DIE LÖSUNG: #1

EINZIGARTIGES PASSWORT AUF DEM GEHÄUSE



DIE LÖSUNG: #1

EINZIGARTIGES PASSWORT AUF DEM GEHÄUSE



DIE LÖSUNG: #2

ERZWUNGENE PASSWORTÄNDERUNG BEI ERSTER BENUTZUNG

osTicket version 1.6 Stable - Basic installation

All fields are required.

osTicket web path and title

Url to osTicket installation on your server and the title.

HelpDesk URL:

HelpDesk Title:

System email

Default system email (e.g support@yourdomain.com) You can change or add more emails later.

Default Email:

Admin user

Min of six characters for the password. You can change or add more users later.

Username:

Password:

Password (again):

Email:

SUPPORTFALLE?

- ❖ Durch ein vergessenes Passwort könnte das Gerät „gebricked“ werden
- ❖ Rücksetzung über Standardprozedur, z.B. Knopf lange drücken beim Einschalten



KONFIGURATION DURCH KONVENTION

- ❖ Standards
- ❖ Von Faulheit und Erfolg guter Ideen
- ❖ **Vom Erfolg der PHP-Programme**
- ❖ Befehle in Shells

VOM ERFOLG DER PHP-PROGRAMME

1. Reinkopieren
2. Aufrufen
3. Fertig

„Schneide nutzlose Begriffe, Methoden und Annahmen
heraus.“

Occams Messer

Geht es noch einfacher?

Geht es **noch** einfacher?

Ist das **wirklich** notwendig?

Einen Raum vollzustellen
ist leicht.

Einen Raum nur mit dem Notwendigen zu befüllen
ist wirklich harte Arbeit.

Richard Lippmann

VOM ERFOLG DER PHP-PROGRAMME

1. Reinkopieren
2. Aufrufen
3. Fertig

Aber wie geht das?

VOM ERFOLG DER PHP-PROGRAMME

1. PHP-Programmierer haben es geschafft Programme fast ohne Konfiguration zum Laufen zu bringen
2. PHP-Programme laufen auf den meisten Webservern ohne weitere Konfiguration
3. Beim ersten Aufruf des Programms (index.php) wird man sofort nach setup.php weitergeleitet
4. Einstellungen des Programms durch den Erst-User = Admin
5. Abspeichern der Config nach config.php das selbst aber keine Ausgabe liefert.
6. Hinweis an **jeden** Benutzer setup.php zu löschen (das tut weh!)
7. Es gibt kein Weiterkommen solange setup.php noch da ist

KONFIGURATION DURCH KONVENTION

- ❖ Standards
- ❖ Von Faulheit und Erfolg guter Ideen
- ❖ Vom Erfolg der PHP-Programme
- ❖ **Befehle in Shells**

BEFEHLE IN SHELLS

- ❖ Was eine Kommandozeile ist
- ❖ das schwarze Fenster in Windows
- ❖ das Terminalfenster in Linux

```
C:\> Eingabeaufforderung
17.10.2015 19:52 <DIR> ..
23.06.2014 15:21 <DIR> .android
27.04.2014 10:37 <DIR> .freemind
16.09.2015 19:19 <DIR> 3D Objects
24.02.2014 11:22 <DIR> Application Da
24.10.2015 10:42 <DIR> Contacts
03.11.2015 16:26 <DIR> Desktop
24.10.2015 10:42 <DIR> Documents
03.11.2015 16:26 <DIR> Downloads
31.10.2015 07:48 <DIR> Dropbox
18.06.2015 06:25 <DIR> Dropbox (Findu
24.10.2015 10:42 <DIR> Favorites
24.10.2015 10:42 <DIR> Links
24.10.2015 10:42 <DIR> Music
16.08.2015 21:42 <DIR> OneDrive
24.10.2015 10:42 <DIR> Pictures
24.10.2015 10:42 <DIR> Saved Games
24.10.2015 10:42 <DIR> Searches
03.11.2015 16:26 <DIR> SkyDrive
31.10.2015 07:49 <DIR> Sync
24.10.2015 10:42 <DIR> Videos
0 Datei(en), 0 Bytes
22 Verzeichnis(se), 198.282.211.328

C:\Users\horshack>
```

BEFEHLE IN SHELLS

- ❖ Man kann große Dinge tun
- ❖ Mit wenigen Befehlen große Bewegungen im Datenfluß anstoßen

```
C:\> Eingabeaufforderung
17.10.2015 19:52 <DIR> ..
23.06.2014 15:21 <DIR> .android
27.04.2014 10:37 <DIR> .freemind
16.09.2015 19:19 <DIR> 3D Objects
24.02.2014 11:22 <DIR> Application Da
24.10.2015 10:42 <DIR> Contacts
03.11.2015 16:26 <DIR> Desktop
24.10.2015 10:42 <DIR> Documents
03.11.2015 16:26 <DIR> Downloads
31.10.2015 07:48 <DIR> Dropbox
18.06.2015 06:25 <DIR> Dropbox (Findu
24.10.2015 10:42 <DIR> Favorites
24.10.2015 10:42 <DIR> Links
24.10.2015 10:42 <DIR> Music
16.08.2015 21:42 <DIR> OneDrive
24.10.2015 10:42 <DIR> Pictures
24.10.2015 10:42 <DIR> Saved Games
24.10.2015 10:42 <DIR> Searches
03.11.2015 16:26 <DIR> SkyDrive
31.10.2015 07:49 <DIR> Sync
24.10.2015 10:42 <DIR> Videos
      0 Datei(en),          0 Bytes
      22 Verzeichnis(se), 198.282.211.328

C:\Users\horshack>
```

BEFEHLE IN SHELLS

- ❖ Die Shell ist ein Programm mit einer Textschnittstelle
- ❖ Einige Befehle sind in der Shell selber eingebaut, z.B. echo, cd
- ❖ alle anderen Befehle werden „gefunden“
- ❖ eine Umgebungsvariable `%PATH%` wird untersucht

BEFEHLE IN SHELLS



DIE PATH VARIABLE

```
C:\Users\horshack>echo %PATH%
C:\Program Files (x86)\ActiveState Komodo Edit 8\;C:\ProgramD
apath;C:\Perl\site\bin;C:\Perl\bin;c:\Program Files (x86)\Int
Program Files\Intel\iCLS Client\;C:\WINDOWS\system32;C:\WINDO
m32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\Progr
l(R) Management Engine Components\DAL;C:\Program Files\Intel\
Engine Components\IPT;C:\Program Files (x86)\Intel\Intel(R)
omponents\DAL;C:\Program Files (x86)\Intel\Intel(R) Managemen
\IPT;C:\Program Files (x86)\Windows Live\Shared;C:\Program Fi
SQL Server\100\Tools\Binn\;C:\Program Files\Microsoft SQL Se
\;C:\Program Files\Microsoft SQL Server\100\DTS\Binn\;C:\PROG
an Files (x86)\Common Files\Acronis\SnapAPI\;C:\Program Files
b;C:\Program Files\OpenVPN\bin
C:\Users\horshack>_
```

BEFEHLE IN SHELLS



DIE PATH VARIABLE - AUFGETEILT

```
C:\Program Files (x86)\ActiveState Komodo Edit 8\  
C:\ProgramData\Oracle\Java\javapath  
C:\Perl\site\bin  
C:\Perl\bin  
c:\Program Files (x86)\Intel\iCLS Client\  
c:\Program Files\Intel\iCLS Client\  
C:\WINDOWS\system32  
C:\WINDOWS  
C:\WINDOWS\System32\Wbem  
...  
C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\  
C:\Program Files\Microsoft SQL Server\100\Tools\Binn\  
C:\Program Files\Microsoft SQL Server\100\DTS\Binn\  
C:\PROGRA~2\Gupta  
C:\Program Files (x86)\Common Files\Acronis\SnapAPI\  
C:\Program Files (x86)\GNU\GnuPG\pub  
C:\Program Files\OpenVPN\bin
```

SCHLUSS



JE KOMPLEXER EIN SYSTEM IST
DESTO MEHR MÜSSEN EINFACHE
SCHNITTSTELLEN DEN ZUGANG
ERLEICHTERN



SCHLUSS



JE KOMPLEXER EIN SYSTEM IST
DESTO MEHR MÜSSEN EINFACHE
SCHNITTSTELLEN DEN ZUGANG
ERLEICHTERN

