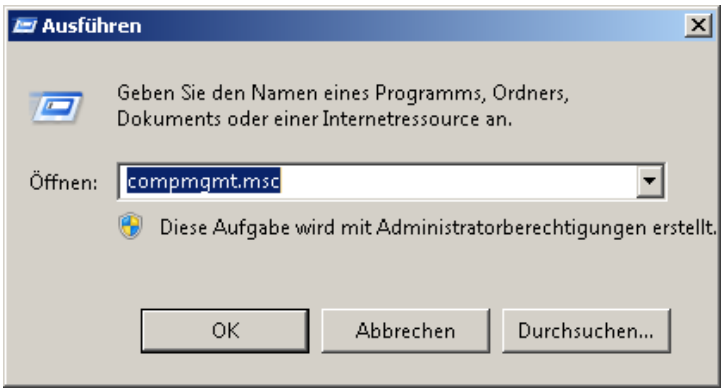
Windows 7/8 - Backdoor

Wenn wir uns in einer peinlichen Situation befinden hätten wir doch gerne mal eine Hintertür parat um unbemerkt verschwinden zu können?!

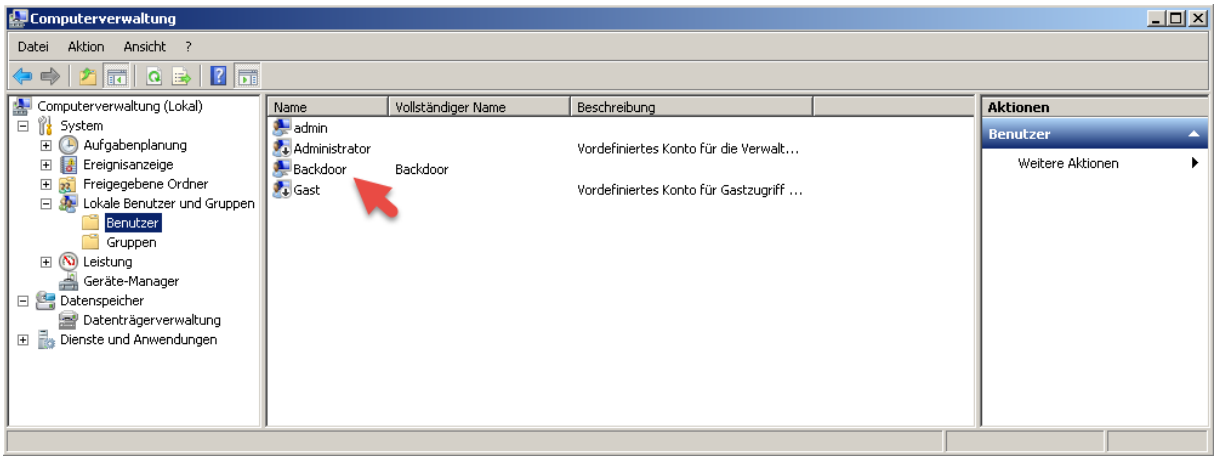
Aber bitte nicht in unserem Betriebssystem!

Mittels eines Registry-Eintrags können wir Benutzer so gut wie unsichtbar machen. Der versteckte Benutzer wäre nur noch über die Computerverwaltung > Lokale Benutzer und Gruppen sichtbar. Er verschwindet aber gänzlich am **Anmeldebildschirm** und in der > **Benutzerkonten-Übersicht**.

Über die Computerverwaltung **Start > Ausführen** und dem Befehl **compmgmt.msc**



Legen wir unter **Lokale Benutzer und Gruppen** einen neuen Benutzer an. Zum Thema passend nennen wir ihn **Backdoor**.



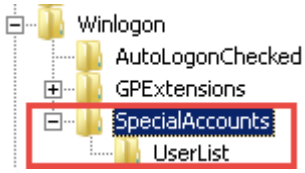
Nun erstellen wir in der Registry einen neuen Eintrag.

Start > Ausführen und dem Befehl **regedit** öffnet sich der Registry-Editor.

Wir fahren zu dem Pfad

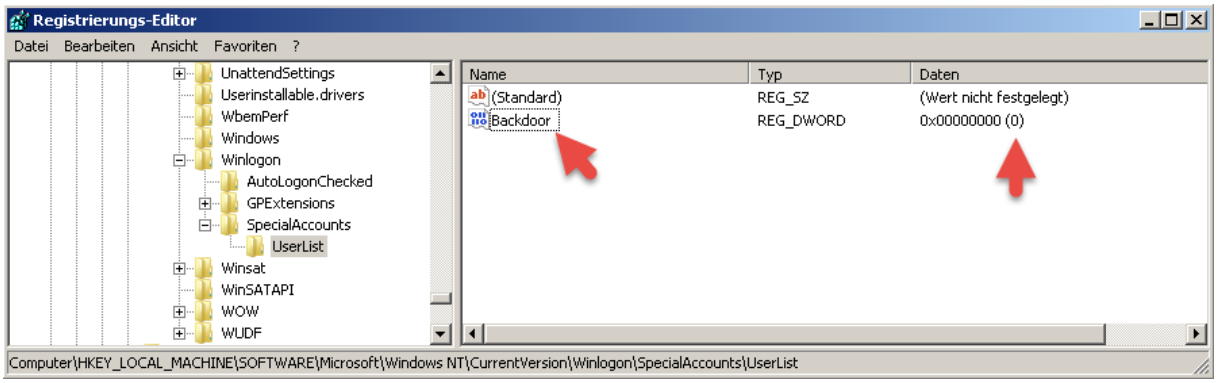
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

und legen unter Winlogon 2 weitere Schlüssel an **SpecialAccounts>Userlist**



Windows 7/8 - Backdoor

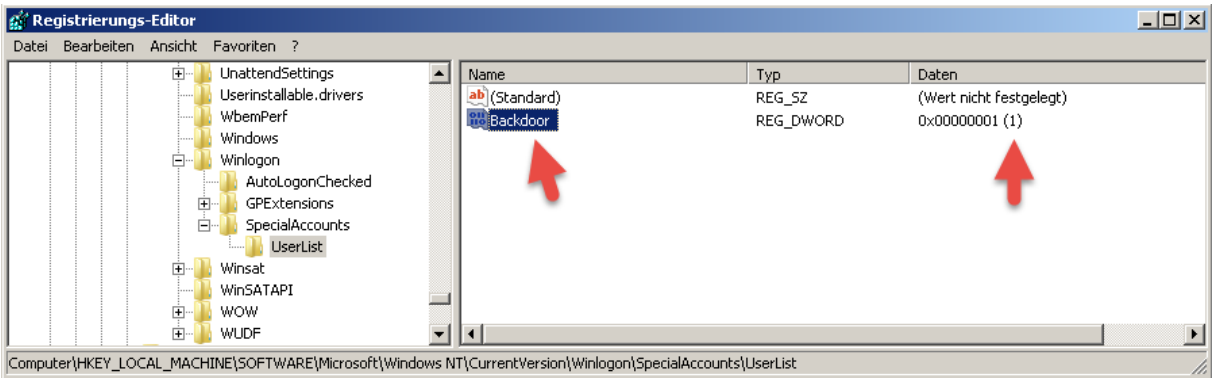
In dem Schlüssel **UserList** legen wir einen neuen **DWORD-Wert (32-Bit)** an und vergeben dem Schlüssel den Namen des Benutzers den wir verstecken wollen, in diesem Fall ist der der User **Backdoor**. Der Wert 0 aktiviert und der Wert 1 deaktiviert die Funktion des Versteckens. Das Ganze sollte dann so aussehen.



Wir melden uns ab und sehen im Anmeldebildschirm nur den Benutzer admin. Klar, der Benutzer **Backdoor** ist **versteckt**.

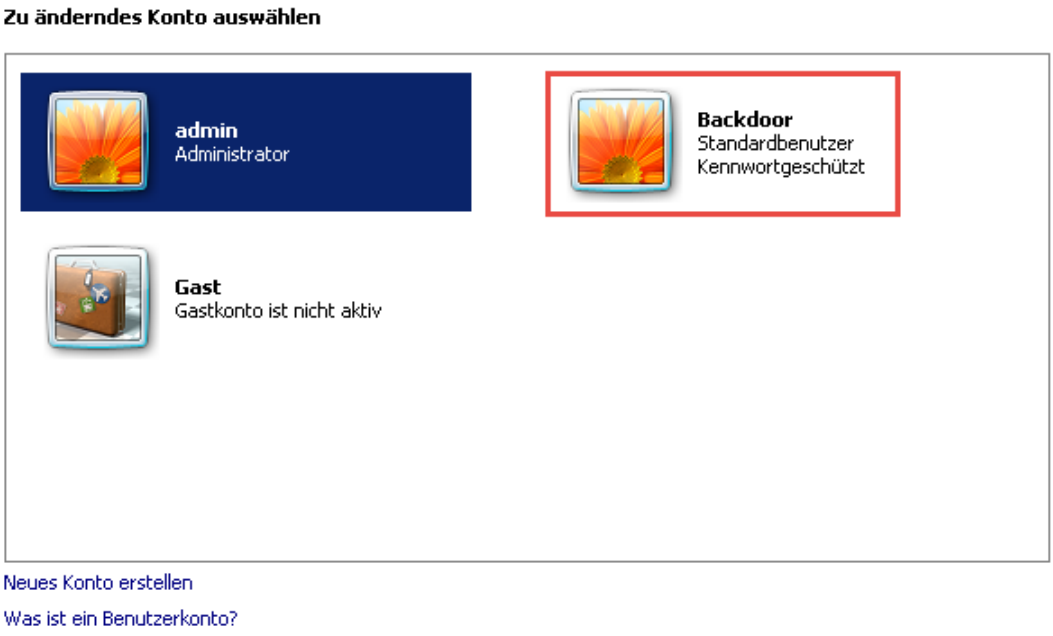
Auch in der Benutzerkonten-Übersicht sehen wir den neuen User nicht.

Wenn wir den Wert jetzt auf 1 stellen, also die Funktion des Versteckens deaktivieren,



So **taucht** der **Benutzer Backdoor** auch wieder im Anmeldebildschirm

sowie in der Benutzerkonten-Übersicht wieder **auf**.



Mit dieser Methode kann sich ein versteckter Benutzer sofern er Mitglied der Gruppe der Administratoren ist, Zugriff auf Ihren Computer verschaffen, ohne das Sie es bemerken werden. Ist doch erschreckend oder?!

Windows 7/8 - Backdoor

Der Registry-Key setzt sich wie folgt zusammen.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList]
"Backdoor"=dword:00000000
```

Kopieren und fügen Sie diesen String in eine Textdatei ein, ändern die Extension von .txt auf .reg, und importieren den Key durch einen Doppelklick in Ihre Registry. Somit ersparen Sie sich den Eingriff und den manuellen Aufwand beim Anlegen der neuen Schlüssel und Werte.

Eine weitere Möglichkeit, liegt in der Manipulation der **Erleichterten Bedienung** **osk.exe**. Die ausführbare EXE Datei finden wir unter dem Pfad **C:\Windows\System32.**

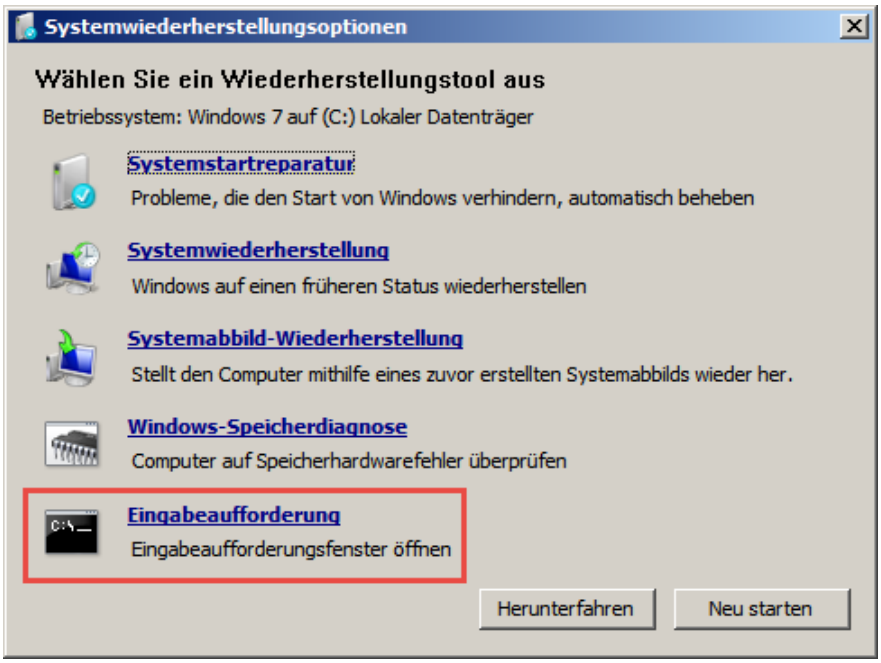
Die Funktion der **Erleichterten Bedienung** (z.B. die Bildschirmtastatur) finden wir unten links auf dem Anmeldebildschirm wieder.

Aber was passiert, wenn wir die **osk.exe** durch die **cmd.exe** austauschen? Richtig, dann öffnet sich nicht mehr der Assistent für die **Erleichterte Bedienung** sondern die Kommandozeile. Über die Kommandozeile wären wir jetzt z.B. in der Lage einen neuen Benutzer anzulegen. Denn die Kommandozeile kommt in dieser Ausgangslage mit administrativen Rechten daher. Das bedeutet im Klartext, den totalen Kontrollverlust über Ihren eigenen Computer.

Und so geht`s.

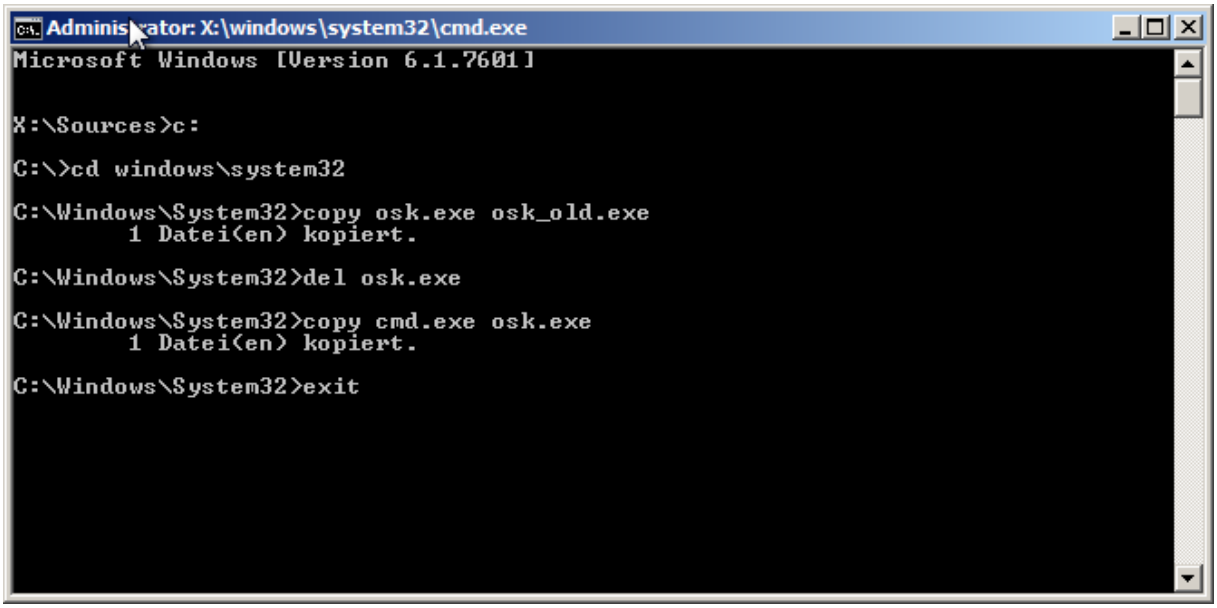
Wir starten den PC mit der passenden Boot-CD und wählen über die **Systemwiederherstellungsoptionen** die **Eingabeaufforderung** aus.

Windows 7/8 - Backdoor



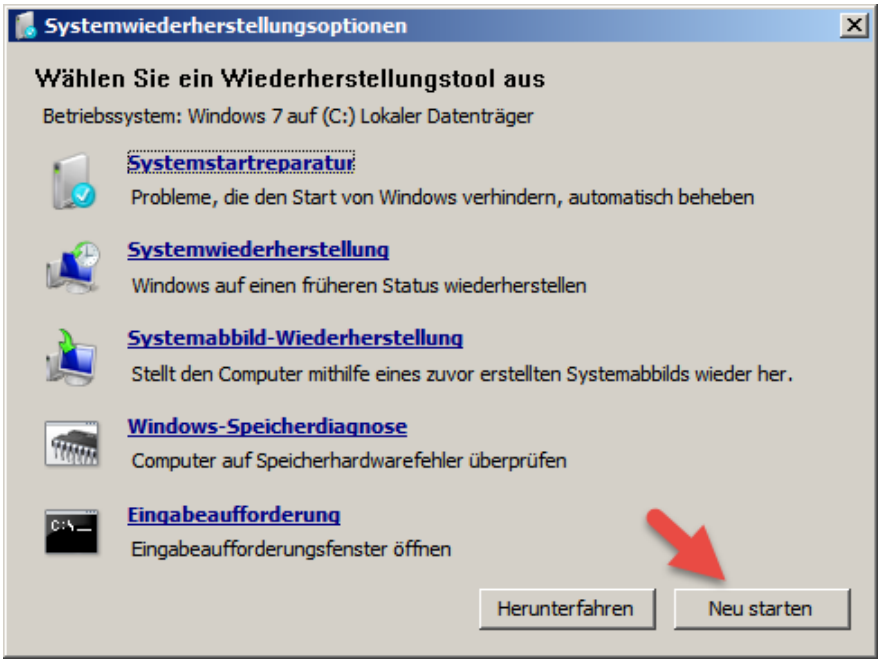
In der Eingabeaufforderung führen wir folgende Batch Befehle aus.

```
c:
cd windows\system32
copy osk.exe osk_old.exe
del osk.exe
copy cmd.exe osk.exe
exit
```



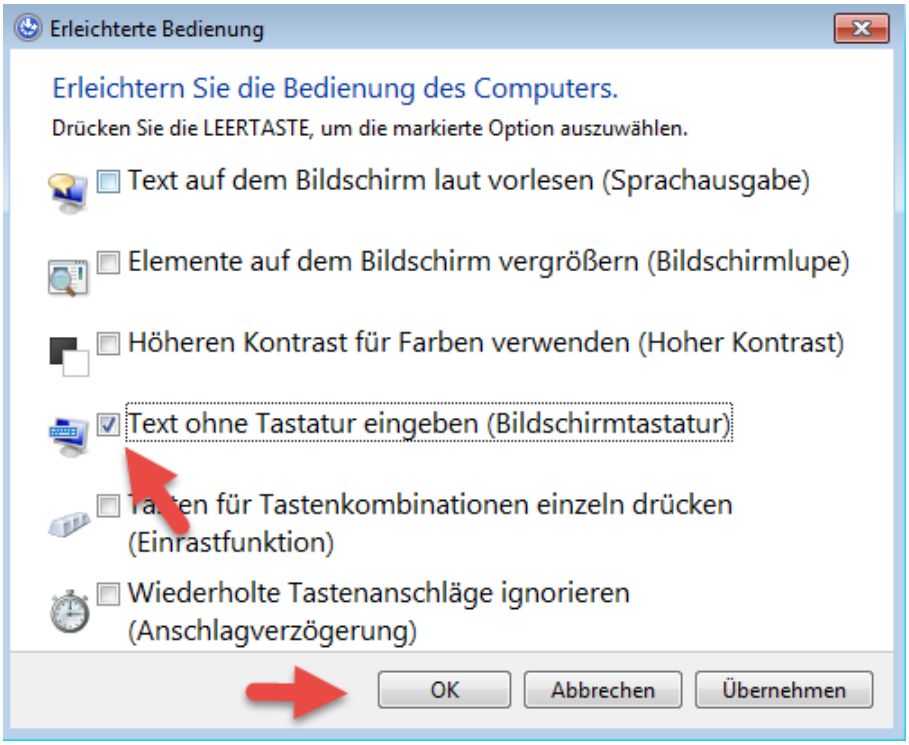
Windows 7/8 - Backdoor

CD/DVD entfernen und **Neu starten**

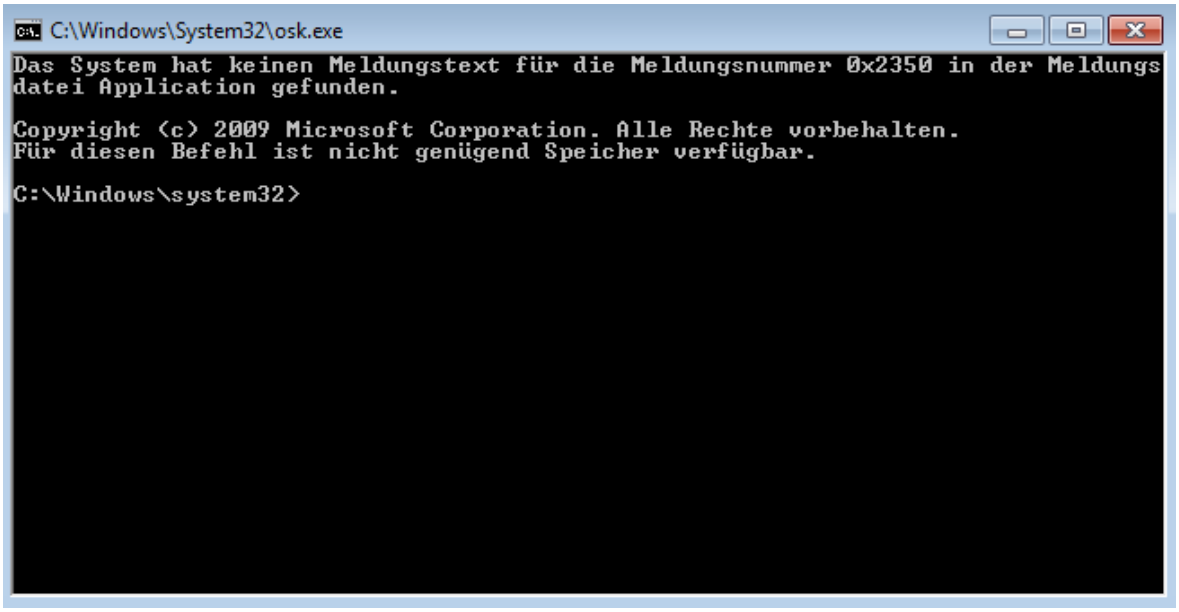


Nach dem Neustart klicken wir auf das Symbol **Erleichterte Bedienung**

Und dann setzen wir den Haken in **Text ohne Tastatur eingeben (Bildschirmtastatur)** und Bestätigen mit **OK.**



Wie oben beschrieben öffnet sich die Kommandozeile mit administrativen Rechten.



Mit dem Befehl **net user backdoor gefahr /add** legen wir einen neuen User an.

Gefolgt von dem Befehl **net localgroup administratoren backdoor /add** fügen wir den Benutzer **backdoor** der Gruppe der lokalen Administratoren hinzu.

Nach einem Neustart kann der **User backdoor** sich mit dem **Password gefahr** anmelden und sein Benutzerkonto verstecken.

Unter Windows 8 wurde eine kleine Hürde eingebaut um die Kommandozeile zu öffnen.

Zum Öffnen der Kommandozeile ist ein Passwort nötig.