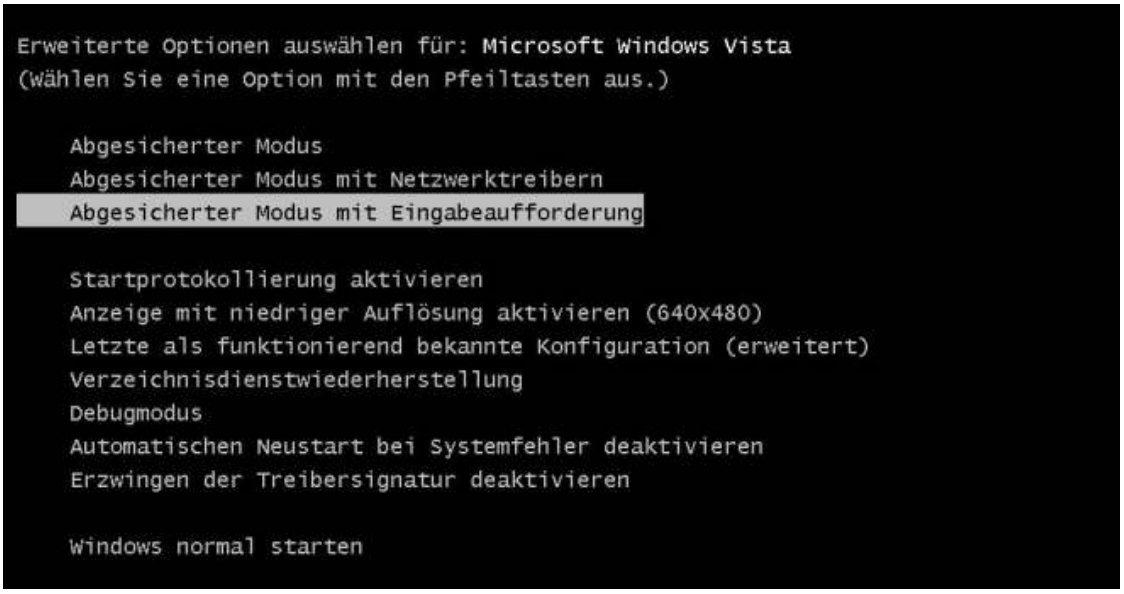
1. Internetverbindung trennen

Netzwerkkabel heraus ziehen, WLAN-/ DSL-Verbindung trennen

2. Windows über die F8-Taste im abgesicherten Modus starten

Rechner einschalten und immer wieder im Sekundentakt (noch bevor das Windows-Logo startet) die Taste **[F8]** drücken bis eine Auswahlliste verschiedener Startvarianten erscheint.

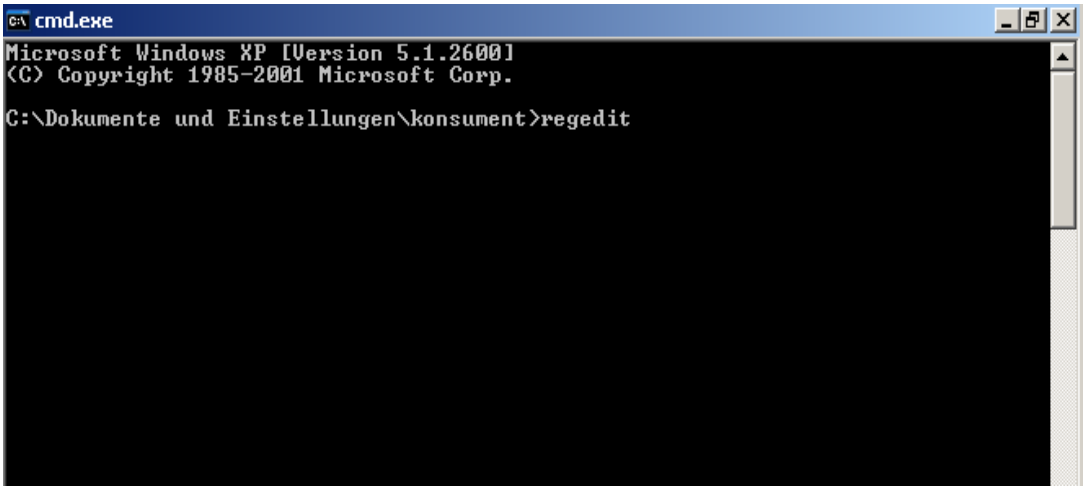
Mit den Pfeiltasten die Option "**Abgesicherter Modus Eingabeaufforderung**" auswählen und mit **[Enter]** bestätigen.



Windows startet nun in einer Art Minimal-Konfiguration.

Der Bildschirm sieht nun nicht wie gewohnt aus. Es öffnet sich die DOS-Eingabeaufforderung (schwarzes Fenster mit Texteingabemöglichkeit).

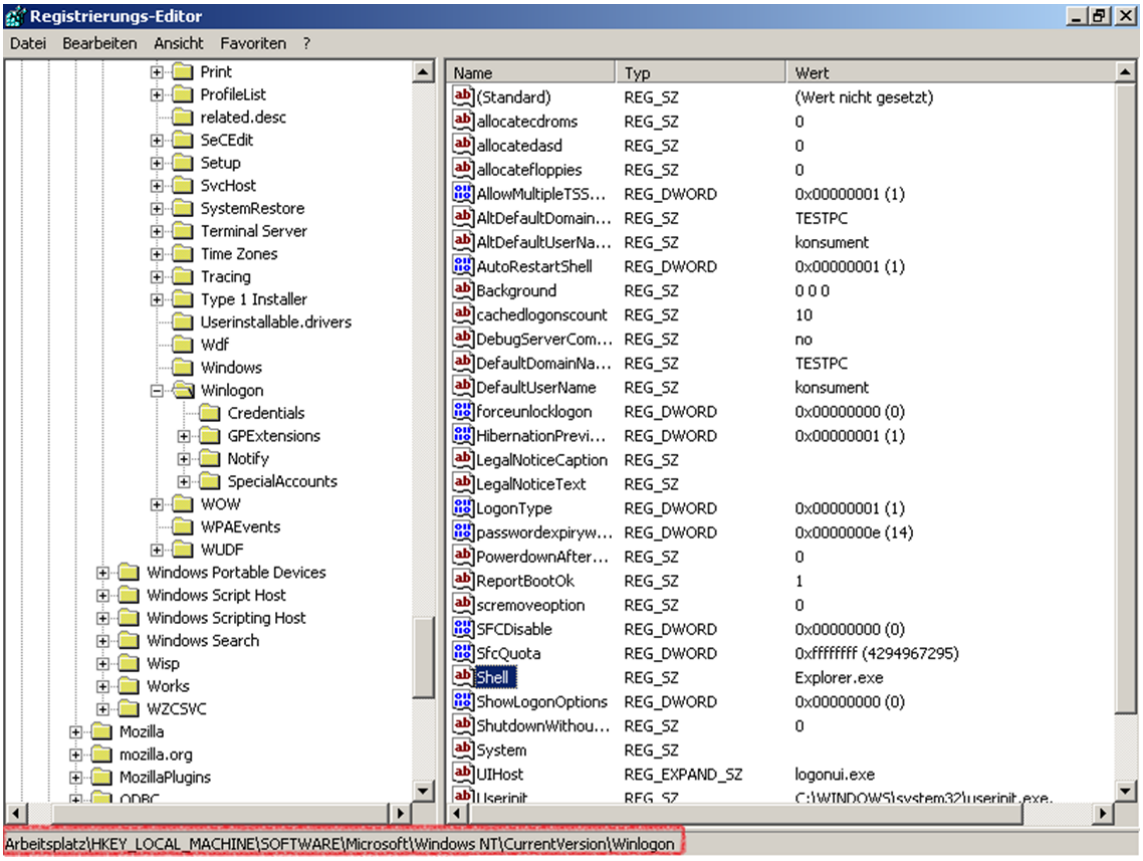
Hier den Befehl ***regedit*** eingeben und **[Enter]** drücken.



Es öffnet sich nun die Windows-Registry, wo eine Änderung vorzunehmen ist.

3. Trojaner finden

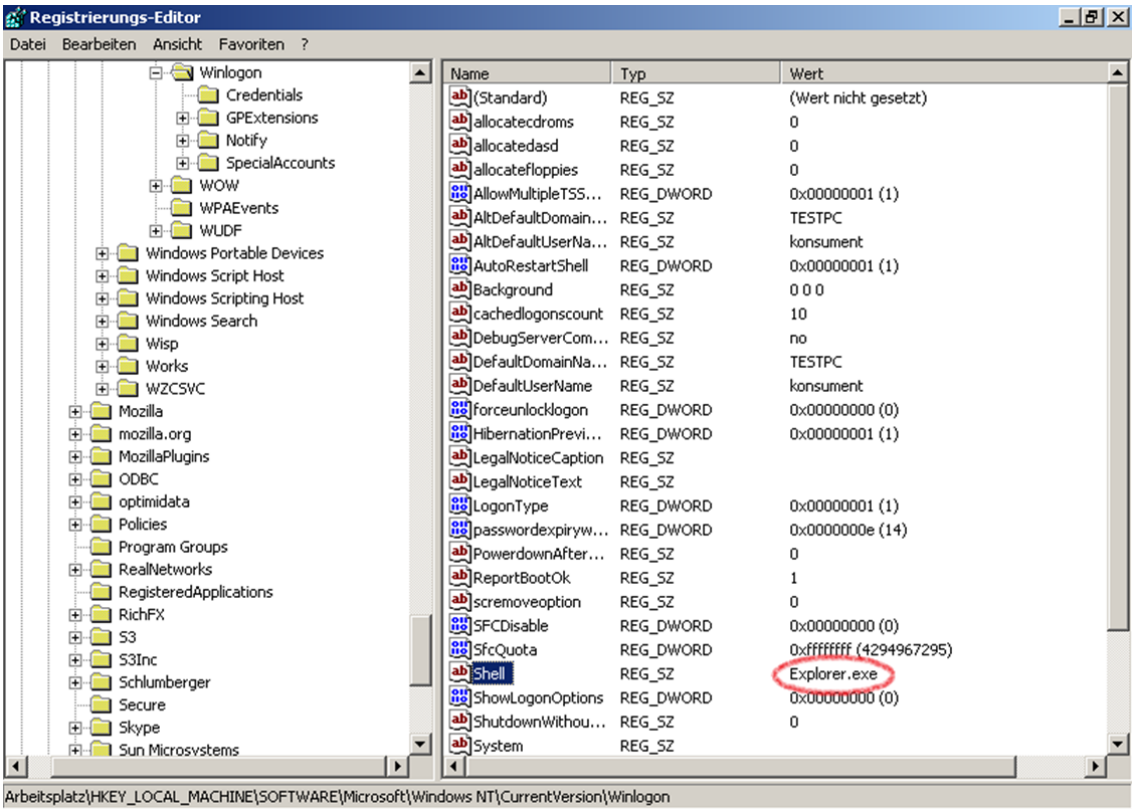
Hier muss durch das Verzeichnis geklickt werden. Ziel ist ***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*** (am Ende ***Winlogon*** direkt auswählen).



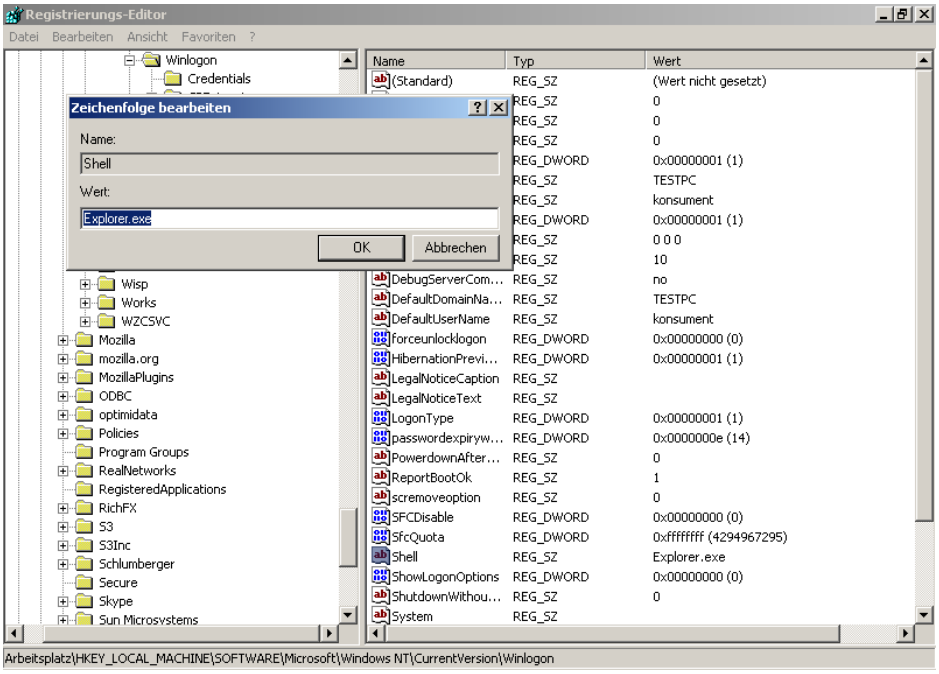
Auf der rechten Fensterseite gibt es einen Schlüssel namens ***Shell*** (→ das ist der BKA-Polizei-Trojaner, andere Schadsoftware kann anders heißen).

Der Wert dieses Schlüssels muss überprüft werden, denn dieser Wert könnte der Pfad zum BKA-Trojaner ***C:\verzeichnis\zur\jashla.exe*** sein.

Den Pfad unbedingt notieren, hier muss später die Datei noch gelöscht werden.



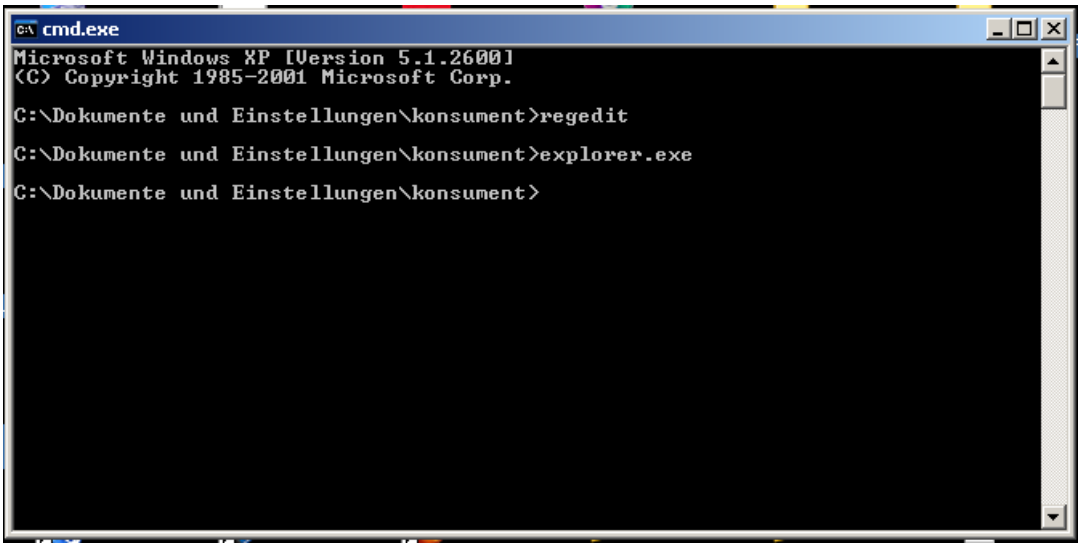
Durch einen Doppelklick auf ***Shell*** öffnet sich ein Fenster, wo der Pfad zum Virus gelöscht und durch ***Explorer.exe*** ersetzt wird. Danach auf **[OK]** klicken und das Registry-Fenster schließen **[x]**.



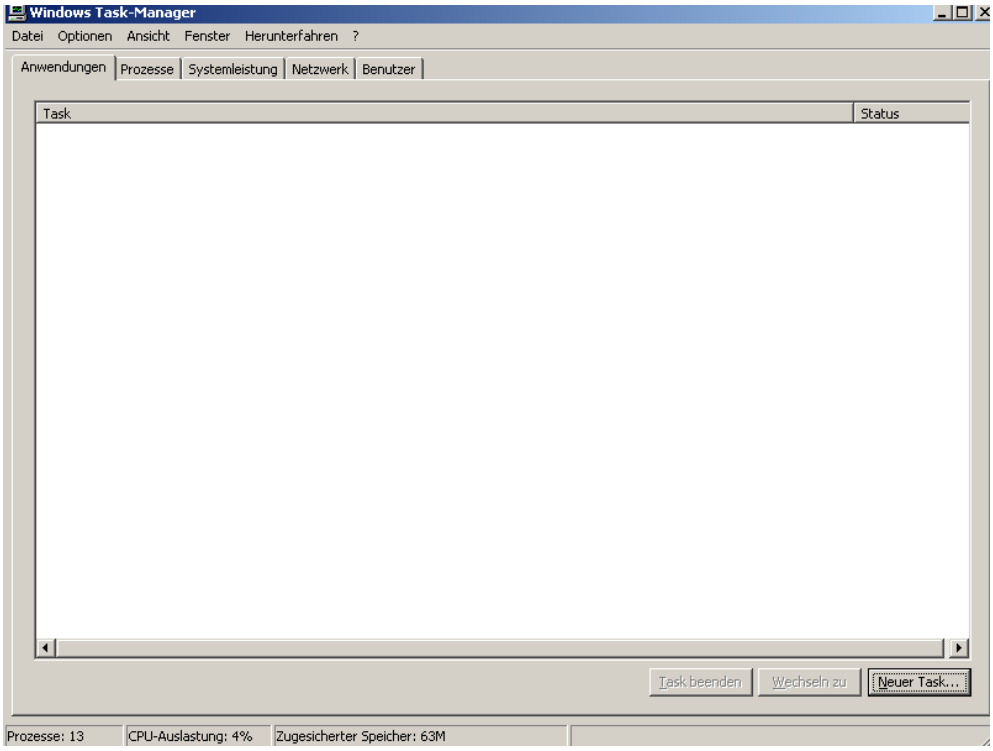
Der Start des Trojaners wird somit verhindert. Jetzt muss dieser aber noch von der Festplatte gelöscht werden.

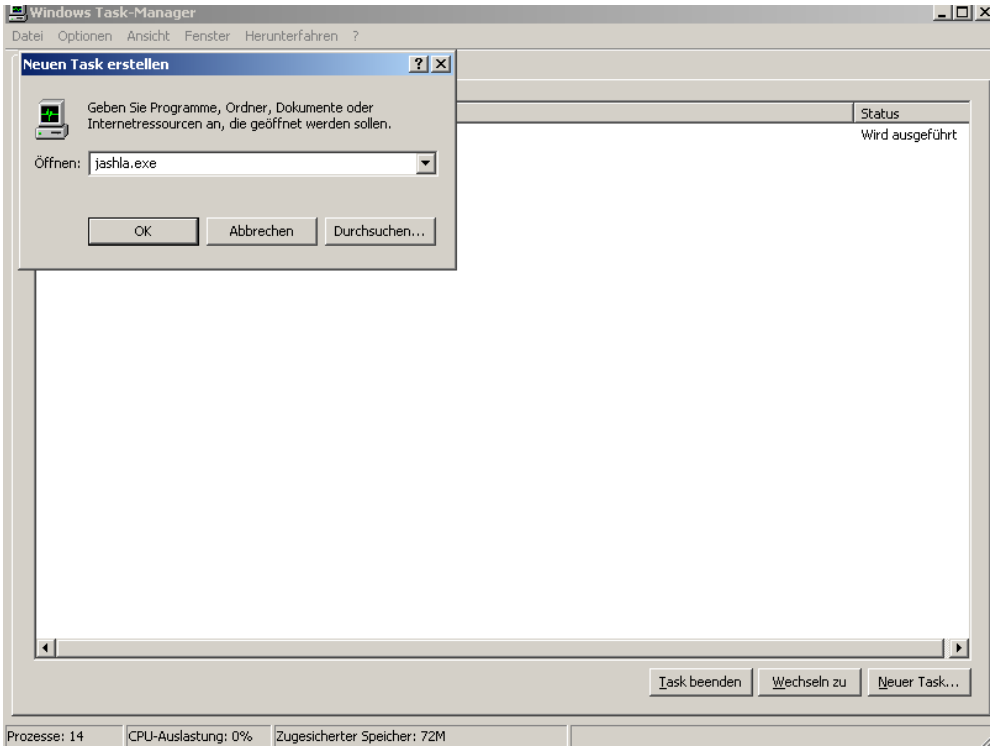
4. Trojaner löschen

Im zuvor schon geöffneten DOS-Eingabefenster ***Explorer.exe*** eingeben. Windows sieht nun fast schon wieder wie gewohnt aus.



Zur ***jashla.exe*** Datei navigieren oder die Windows-Suche nutzen, um die ***jashla.exe*** auf der Festplatte zu finden. Datei löschen. Außerdem kann die Datei mittels Tast-Manager (**[STRG] + [ALT] + [ENTF]**) geöffnet werden, in dem unter „**Anwendungen**“ auf „**Neuer Task**“ geklickt und ***jashla.exe*** eingegeben wird.





Nun muss zum zuvor notierten Pfad navigiert und die ***jashla.exe***-Datei gelöscht werden.