

**LAS-WEBSERVICE.COM**

Ihre Homepage & Ihr Onlineshop in guten Händen...  
...bei Ihrer Full-Service WEB-Agentur am Ammersee!

LAS-Webservice ■ Aalstrasse 9 ■ D-82266 Inning a.A.

**Achtung bitte beachten!**  
**Die Anleitung bezieht sich auf**  
**WINDOWS XP.**

**Inzwischen sind neuere Varianten aufgetreten die wir selbst noch nicht "live" erlebt haben - hier funktioniert die Anleitung eventuell nicht.**

Bitte haben Sie Verständnis dafür, dass wir KEINEN Support leisten können und diese Anleitung kostenlos für Betroffene zur Verfügung stellen. Einige Tipps zu neueren Varianten und anderen Windows-Versionen finden Sie auch hier:

<http://www.las-webservice.com/edv-service/tipps--tricks---hardware/entfernen-des-bundespolizei-trojaner/index.html>

- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VB & VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

**Lothar Armbruster**  
**Webservice**

Aalstrasse 9  
D-82266 Inning a.A.

☎ +49 (8143) 44 46 46

☎ +49 (8143) 93 15 15

✉ Mail: info@las-webservice.com

UST-Nr.: DE177660035

Schritt für Schritt Anleitung  
zum **entfernen** des:

**„Bundespolizei-Trojaner“ auf Windows XP**

Ich staunte nicht schlecht als mich ein Bekannter anrief und mir sagte er habe eine Nachricht auf dem Bildschirm – angeblich von der Bundespolizei und er solle 100 Euro zahlen damit sein Rechner wieder entsperrt wird.

Erst musste ich lachen. Mir wurde aber recht schnell klar, dass es kein Scherz war – denn diese Meldung war nicht mehr wegzubekommen und blockierte den kompletten Rechner.

Ich sah mir das ganze an und staunte nicht schlecht – denn so was kenne ich bisher nur aus Computerzeitschriften und Viren-Newslettern – jetzt aber wurde ich direkt mit diesem „Ding“ konfrontiert.

www.LAS-Webservice.com

Eine Erpressung – voll mit Rechtschreibfehlern und angeblich auch noch von der Bundespolizei.

Das dieses ein Fake ist war klar, aber wie bekommt man wieder einen Zugriff auf den Rechner, der ja sofort blockiert und nur noch diese Meldung anzeigt?

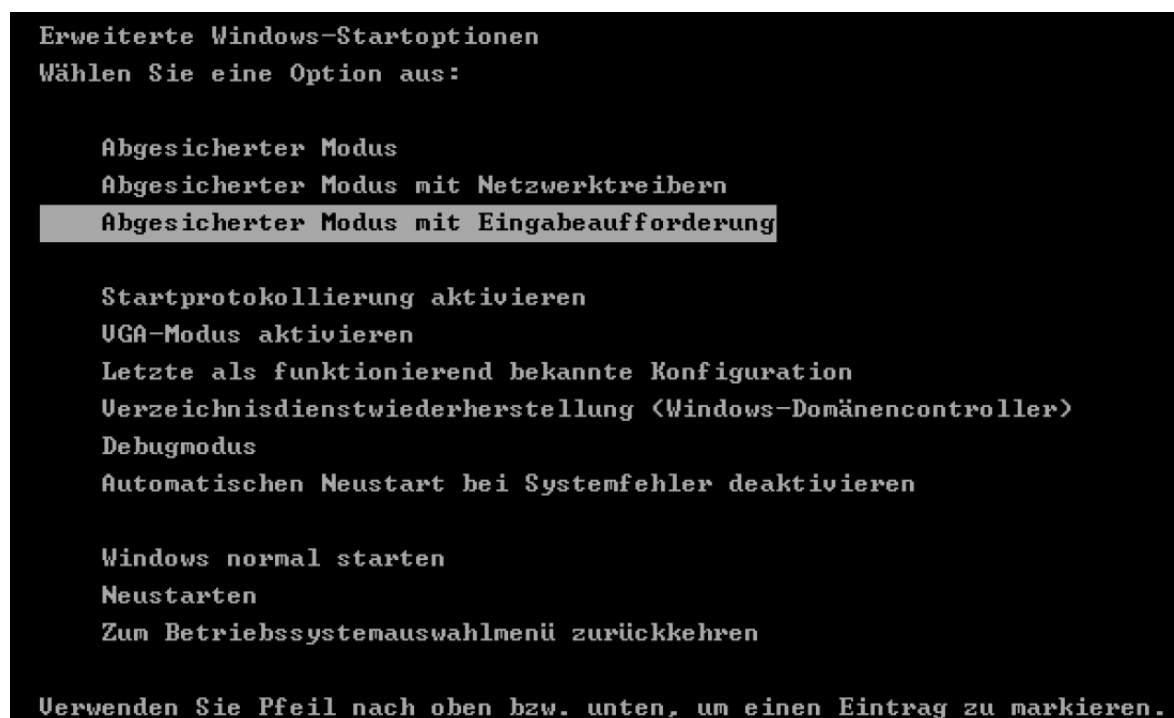
Mehrere Versuche diesen Schädling zu entfernen schlugen zuerst fehl. Die Meldung kam immer wieder nach dem Starten - auch im Abgesicherten Modus und blockierte alles:

- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

## **So klappts mit dem Entfernen:**

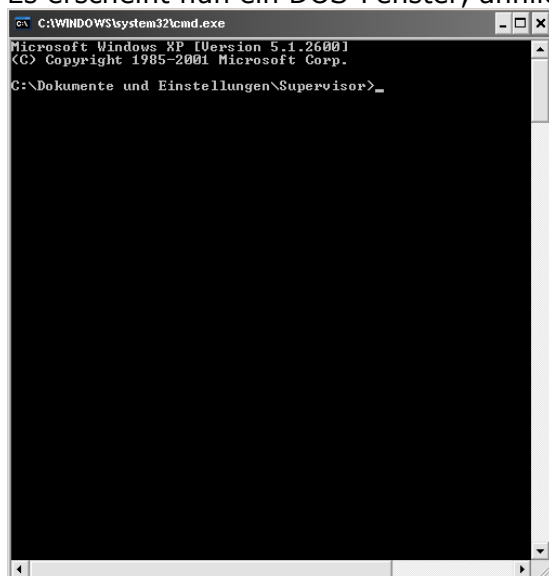
1. Atmen Sie jetzt erst einmal durch und bleiben Sie ruhig, denn mit dieser Anleitung müsste alles danach auch bei Ihnen wieder „normal“ funktionieren.
2. Kappen Sie die Verbindung zum Internet (DSL-Router) und ziehen Sie das Netzkabel.
3. Schalten Sie den Rechner aus.
4. Schalten Sie den Rechner ein und drücken jetzt immer wieder die **[F8]** Taste bis folgender Bildschirm erscheint. *(Wenn das Windows Logo erscheint, bei Punkt 3 neu beginnen).*

Sie haben jetzt ein Auswahlmenü bei dem Sie mit den CURSOR-Tasten die Variante: **„Abgesicherter Modus mit Eingabeaufforderung“** auswählen und mit ENTER bestätigen



Windows wird nun in einer minimalen Art gestartet. Es kann sein dass Sie Ihrem Benutzernamen und Ihr Kennwort eingeben müssen.

5. Es erscheint nun ein DOS-Fenster, ähnlich wie dieses:

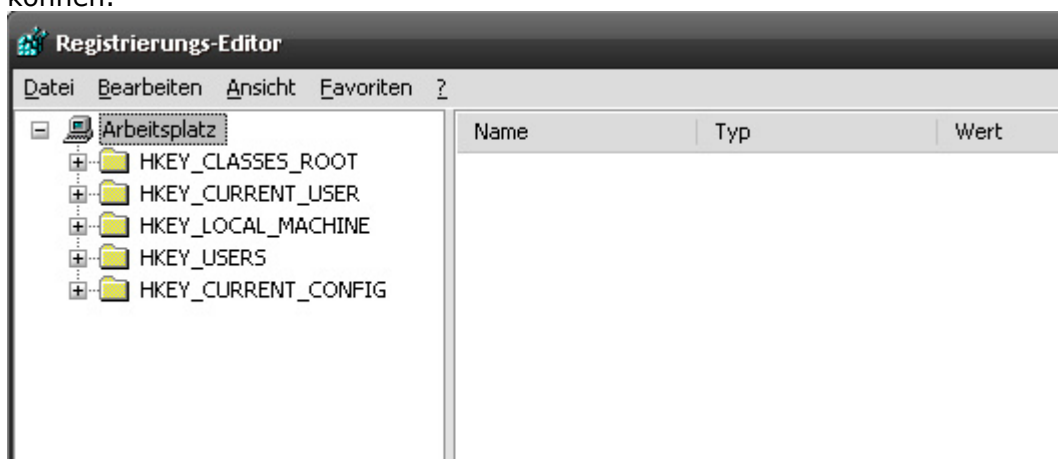


- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

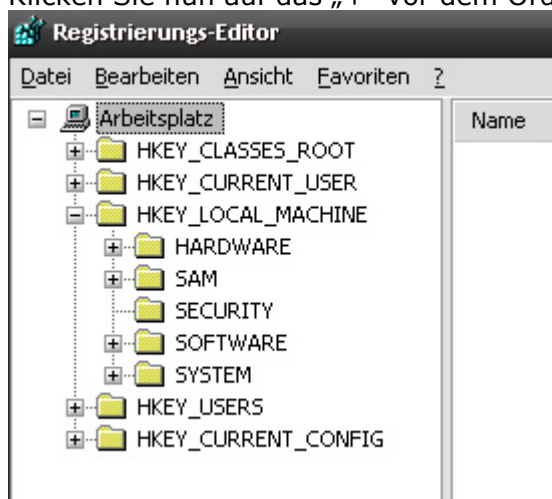
6. Geben Sie nun über die Tastatur den Befehl: **regedit** ein und bestätigen Sie Ihre Eingabe mit der **ENTER**-Taste

```
C:\Dokumente und Einstellungen\Supervisor>regedit_
```

7. Nun öffnet sich der **WINDOWS-REGISTRIERUNGS-EDITOR** bei dem Sie nun wie folgt zum entsprechenden Eintrag gelangen um dem Trojaner die Grundlage zu entziehen, dass er sofort aktiv wird und Sie den Rechner wieder bedienen können.



8. Klicken Sie nun auf das „+“ vor dem Ordner: **HKEY\_LOCAL\_MACHINE**



- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

9. Klicken Sie nun auf das „+“ vor dem Ordner: **SOFTWARE**

10. Suchen Sie nun den Ordner **MICROSOFT** und klicken Sie hier auf das „+“ vor dem Ordner

11. Suchen Sie nun den Ordner **WINDOWS NT** und klicken Sie hier auf das „+“ vor dem Ordner

12. Suchen Sie nun den Ordner **CurrentVersion** und klicken Sie hier auf das „+“ vor dem Ordner.

13. Klicken jetzt Sie **direkt** auf den Ordner: **WINLOGON** Sie sehen jetzt einige Registrierungsschlüssel.

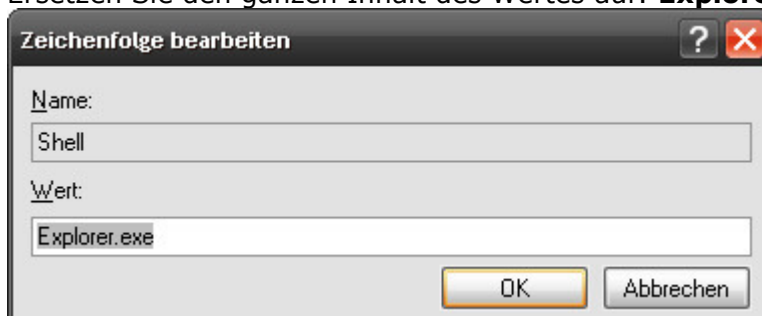
14. Nun einen **DOPPEL-Klick** auf den Schlüssel: **SHELL** um hier einen Wert zu ersetzen. Es wird ein Fenster geöffnet:



Der Inhalt dieses Wertes kann abweichen, so kann z.B. auch ein Wert beinhaltet sein wie: C:\Verzeichnis1\Verzeichnis2\LOKALE~1\Temp\**jashla.exe**

**Sie müssen sich nun diesen Wert unbedingt notieren, damit Sie den Trojaner nachher auch finden und löschen können. Das ist der Speicherort und der Trojaner** (in unserem Fall war es wpbt0.dll).

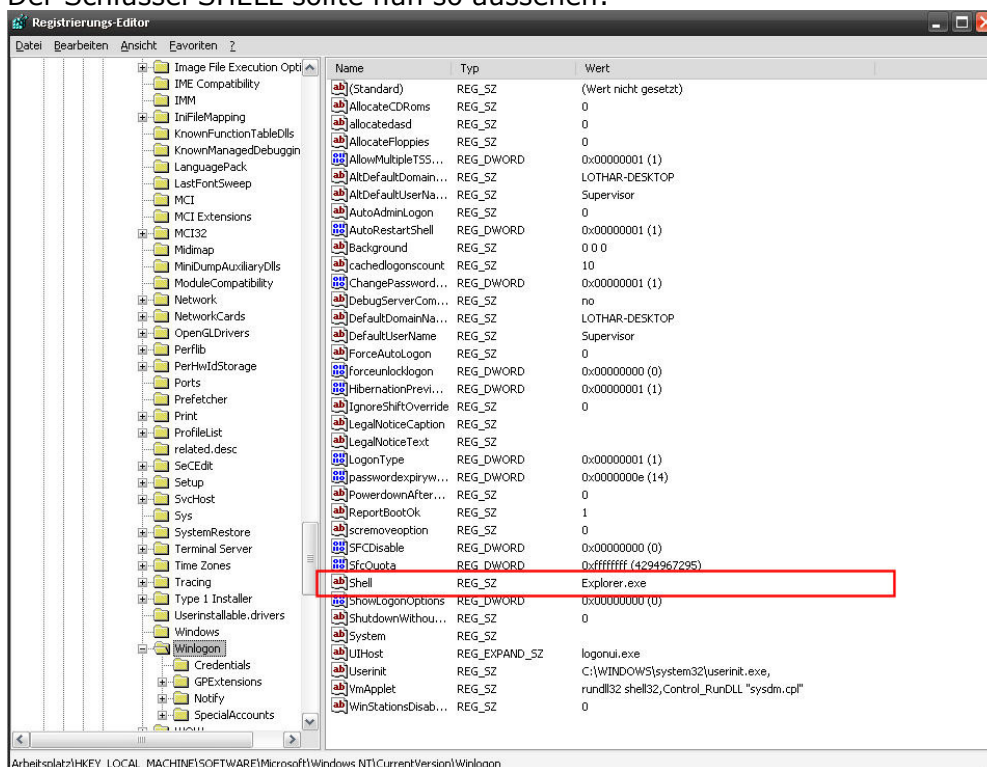
15. Ersetzen Sie den ganzen Inhalt des Wertes auf: **Explorer.exe**



- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

**Klicken Sie nun auf OK**

Der Schlüssel SHELL sollte nun so aussehen:



Schliessen Sie jetzt den Registrierungs-Editor [**x**]

Damit haben Sie dem Trojaner die Möglichkeit entzogen dass er nach dem Starten des Rechners sofort aktiviert wird. Aber er ist noch nicht entfernt.

16. Geben Sie jetzt im DOS-Eingabefenster den Befehl: **Explorer.exe** ein und bestätigen mit **ENTER**.
17. Suchen Sie nun anhand Ihrer Notiz aus Punkt 14. die entsprechende Datei und löschen diese endgültig mit gedrückter [**Unschalttaste**] und [**ENTF**].
18. Starten Sie jetzt Ihren Rechner neu und ganz normal.



- Webdesign & Hosting
- Digitale Bildbearbeitung
- CMS-Lösungen
- VBA-Programmierung
- e-Commerce-Systeme
- Netzwerktechnik
- EDV & Bürooptimierung

Wenn der Rechner nicht wie gewohnt hochfährt haben Sie sicher etwas übersehen – gehen Sie meine Anleitung noch einmal komplett durch, Sie müssen was übersehen haben.

Startet der Rechner wieder ganz normal sollten Sie auf jeden Fall mit einer aktuellen Antivirensoftware diesen überprüfen.

**Wir empfehlen hier immer eine Vollversion.**

Kurioserweise hatte unser Bekannter eine Vollversion, die aber vermutlich aufgrund eines fehlgeschlagenen Updates nicht aktiv war. Also überprüfen Sie daher auch immer ob Ihr Virens Scanner aktiviert ist.

Läuft alles – wieder – dann dürfen Sie jetzt Ihren Rechner auch wieder mit dem Internet verbinden.

Bis der Rechner wieder komplett sauber und aufgeräumt war benötigte ich insgesamt 8 Stunden, inklusive Neuinstallation des Virens Scanners und komplett-Check. Bei dieser Gelegenheit wurde auch fast 2 GB Datenmüll entsorgt und das gesamte Dateisystem bereinigt.

Mit der Anleitung sollten Sie schneller ans Ziel kommen.

Der Rechner läuft wieder wie eine 1.