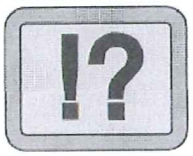


So spüren Sie die Verstecke in der Registry auf

Autostart und Co.

Die Registry ist das optimale Versteck für Eintragungen, die Spionageprogramme zum automatischen Start oder Ausführen von gefährlichen Funktionen benötigen. Die Suche in den tief geschachtelten Strukturen der Registrierungsdatenbank gestaltet sich schwierig, doch es gibt nur einige Pfade, in denen sich Spionageprogramme eintragen.

Über Start und Ausführen... geben Sie den Befehl „regedit" ein, um den Registrierungsdatenbankeditor aufzurufen.

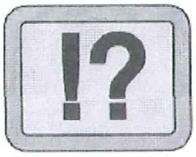
Die folgende Liste zeigt die wichtigsten Pfade, über die Spionageprogramme automatisch gestartet werden können. Prüfen Sie diese Eintragungen zuerst:

Autostarteinträge in der Registry

```
HKEY_LOCAL_MACHINE\Software\Microsoft\...
  ... Windows\CurrentVersion\RunServices\
HKEY_LOCAL_MACHINE\Software\Microsoft\...
  ...Windows\CurrentVersion\RunServicesOnce\
HKEY_LOCAL_MACHINE\Software\Microsoft\...
  ...Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\Software\Microsoft\...
  ...Windows\CurrentVersion\RunOnce\
HKEY_LOCAL_MACHINE\Software\Microsoft\...
  ...Windows\CurrentVersion\RunOnceEx\
HKEY_LOCAL_MACHINE\Software\Policies\...
  ...Microsoft\Windows\System\Scripts\Startup
HKEY_LOCAL_MACHINE\Software\Microsoft\
...Windows\CurrentVersion\ShellServiceObjectDelayLoad\
```

Benutzerabhängige Autostarteinträge

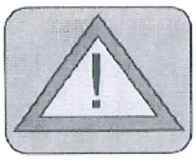
```
HKEY_USERS\DEFAULT\Software\Microsoft\...
  ...Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\...
  ...Windows\CurrentVersion\Run\
HKEY_CURRENT_USER\Software\Microsoft\...
  ...Windows\CurrentVersion\RunOnce\
HKEY_CURRENT_USER\Software\Microsoft\...
  ...Windows\CurrentVersion\RunServices\
HKEY_CURRENT_USER\Software\Microsoft\...
  ...WindowsNT\CurrentVersion\Windows\Run\
```



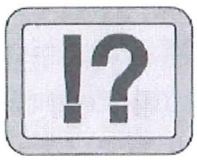
```
HKEY_CURRENT_USER\Software\Microsoft\...
  ...WindowsNT\CurrentVersion\Load\
HKEY_CURRENT_USER\Software\Policies\...
  ...Microsoft\System\Scripts\

HKEY_CLASSES_ROOT\exefile\shell\open\command\
HKEY_CLASSES_ROOT\comfile\shell\open\command\
HKEY_CLASSES_ROOT\batfile\shell\open\command\
HKEY_CLASSES_ROOT\htafile\Shell\Open\Command\
HKEY_CLASSES_ROOT\piffile\shell\open\command\

HKEY_LOCAL_MACHINE\Software\CLASSES\...
  ...batfile\shell\open\command\
HKEY_LOCAL_MACHINE\Software\CLASSES\...
  ...comfile\shell\open\command\
HKEY_LOCAL_MACHINE\Software\CLASSES\...
  ...exefile\shell\open\command\
HKEY_LOCAL_MACHINE\Software\CLASSES\...
  ...htafile\Shell\Open\Command\
HKEY_LOCAL_MACHINE\Software\CLASSES\...
  ...piffile\shell\open\command\
```

Achten Sie in den angegebenen Pfaden auf alle ausführbaren Dateien. Sie erkennen diese an den Dateiendungen „.COM“ oder „.EXE“. Dahinter verbergen sich häufig Spionageprogramme, aber auch normale Programme, die über diesen Eintrag automatisch geladen werden.

Ausführbare Dateien sind verdächtig



Bevor Sie einen verdächtigen Eintrag löschen, sollten Sie den Pfad bzw. den Eintrag unbedingt sichern. Ansonsten funktionieren vielleicht andere Programme nicht mehr ordnungsgemäß.



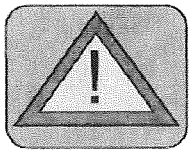
Der Registrierungseditor verfügt dafür über eine komfortable Funktion, um Veränderungen an der Registry durchzuführen und auch wieder rückgängig zu machen. Über „**Datei**“ und „**Exportieren**“ können Sie Teile der Registry auslagern, um diese beispielsweise zu sichern, und über „**Importieren**“ Registry-Änderungen bequem einlesen. Wenn Sie einen Teil der Registry exportieren, so legt der Registrierungseditor eine Datei mit der Endung „.REG“ auf Ihrer Festplatte an. Den Dateinamen selbst können Sie frei wählen.

Im- und Exportfunktion im Registrierungseditor

Kontrollieren Sie Ihren Browser auf böse Objekte

BHO = Browser Helper Objekts

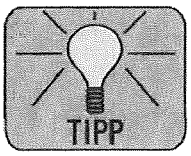
BHO steht für Browser Helper Objects. Auch hier nisten sich Spionageprogramme gerne ein. Diese Programme sind schwer ausfindig zu machen, denn:



- Diese Spyware wird automatisch mit dem Explorer gestartet und benötigt keine Eintragungen in der Registry oder in einem Autostart.
- Diese Spyware wird nicht als eigener Prozess geführt und kann somit nur schwer enttarnt werden.
- Auf diese Spyware reagiert nicht einmal eine Firewall, weil die Spyware über den Internet Explorer die Informationen nach außen gibt.

Service Pack 2 für den IE

Erst mit dem Internet Explorer 6 mit Service Pack 2 haben Sie eine Kontrollmöglichkeit über die BHO.



Haben Sie eine ältere Version des Internet Explorers im Einsatz, so können Sie die vorhandenen BHOs über die Registry überprüfen. Sie finden diese unter dem Pfad „HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\BrowserHelperObjects\".

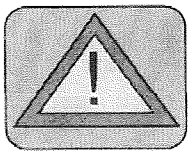
Schädliche Prozesse aufspüren und eliminieren

Der Task-Manager ist ungeeignet

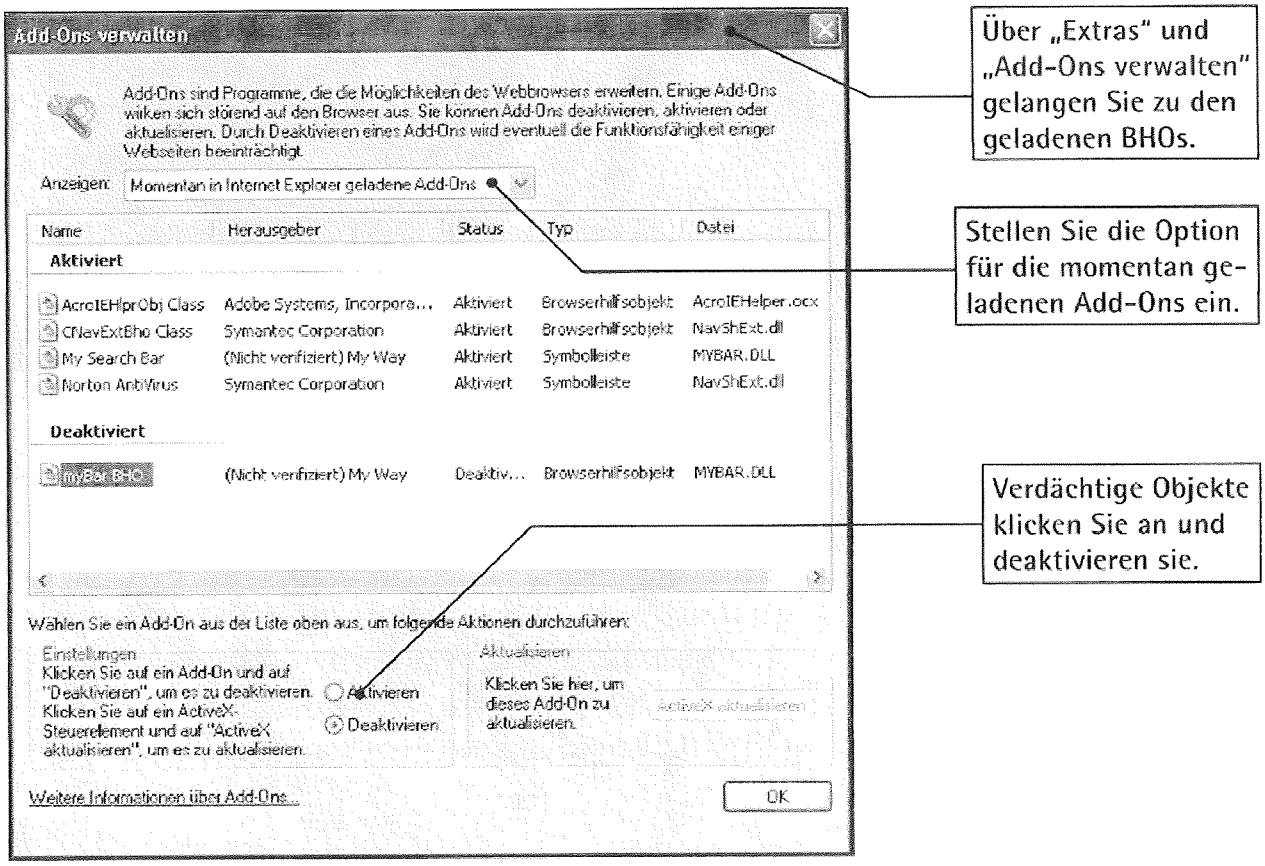
Ausgeführte Programme erscheinen als Prozess in der Prozessliste. Mit Strg+Alt+Entf können Sie den Task-Manager aufrufen und alle aktiven Prozesse einsehen. Leider kennen einige Spionageprogramme diesen Trick und werden erst gar nicht im Task-Manager aufgelistet.

Besser: Process Viewer oder Security Taskmanager

Abhilfe schaffen hier Zusatz-Tools wie „Process Viewer" oder „Security Taskmanager". Letzteres, führt sogar eine Sicherheitsprüfung aus und bewertet die Gefährlichkeit der einzelnen Prozesse.



Es reicht nicht, wenn Sie eine Task einfach nur beenden. Sie müssen die dazugehörigen Dateien ebenfalls löschen. Viele Spionageprogramme sind darauf vorbereitet und schützen sich gegenseitig mit voneinander abhängigen Tasks. In diesem Fall starten Sie den PC im abgesicherten Modus und löschen dann die verdächtigen Dateien. Zur Sicherheit sollten Sie die Dateien vorher umbenennen und erst dann löschen, wenn alle Anwendungen noch einwandfrei funktionieren.



Die Verwaltung der BHOs im Internet Explorer 6

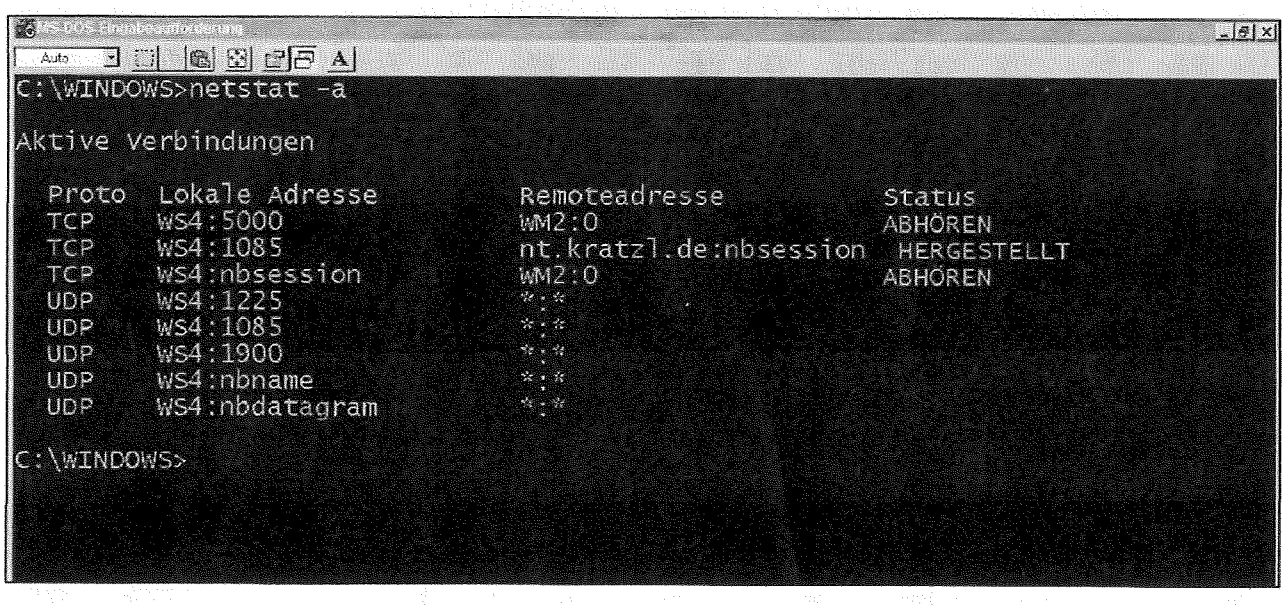
Professionelle Suche nach Schädlingen mit NETSTAT

Der schnelle Check

Die Ports Ihres PCs können Sie schnell und einfach prüfen. Öffnen Sie dazu ein DOS-Fenster über die „MS-DOS-Einga-

beaufforderung“ beziehungsweise „Eingabeaufforderung“ unter Windows 2000/XP.

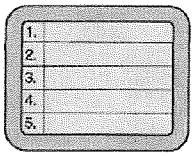
Geben Sie dann den Befehl „netstat -a“ ein und lösen sie ihn mit ↵ aus.



So „horchen“ Sie die offenen Ports ab

Erst offline, dann online

Die Abfrage wird dann interessant, wenn Sie zuerst ohne Online-Verbindung prüfen, welche Ports offen, also auf „Abhören“ eingestellt sind. Bauen Sie dann eine Internetverbindung auf und kontrollieren Sie die offenen Ports erneut. Mit dieser Methode decken Sie nach einiger Beobachtungszeit auch Spionagesoftware auf. Öffnen Sie dazu ein verdächtiges Programm und kontrollieren Sie anschließend wieder die Ports.



Der Kampf gegen Spionagesoftware geht weiter. Solange in den Microsoft-Produkten immer neue Sicherheitslücken entdeckt werden, wird es auch weiterhin Spionageprogramme geben, die diese Lücken ausnutzen. Oft es mühsam, den Eindringling aufzuspüren und zu eliminieren. Viele Anwender greifen deshalb auf ein Image zurück, das in kürzester Zeit installiert werden kann. Somit steht ihnen stets schnell wieder ein sauberes System zur Verfügung.