

# Security Task Manager

Benutzerhandbuch



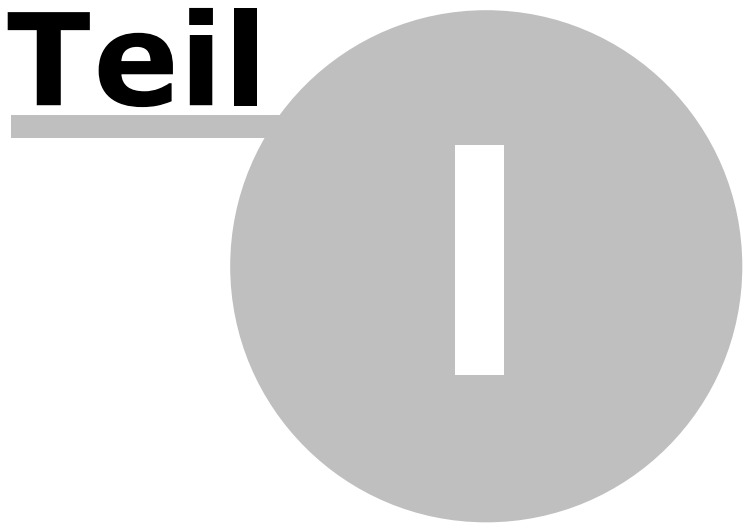
Security Task Manager erkennt potentiell gefährliche Prozesse, welche den PC überwachen oder langsam machen

# Inhaltsverzeichnis

<b>Teil I Was kann der Security Task Manager?</b>	<b>4</b>
<b>Teil II Arbeiten mit dem Security Task Manager</b>	<b>6</b>
Überblick .....	6
Anzeigen der Prozess Eigenschaften .....	6
Anzeigen von weiteren Eigenschaften (Google Suche) .....	7
Beenden eines Prozesses .....	7
Quarantäne-Ordner .....	7
Drucken der Prozess Liste .....	8
Exportieren der Prozess-Liste .....	8
Kommentar und eigene Bewertung zu einem Prozess .....	8
Überprüfen von Änderungen an Hosts Datei .....	8
Ändern der Sprache .....	9
<b>Teil III Grundlagen</b>	<b>11</b>
Risiko-Bewertung der Prozesse .....	11
Prozess Typen .....	12
Wie Sie das Security Task Manager Team erreichen .....	12
Deinstallieren .....	12
<b>Teil IV Schutz mit SpyProtector</b>	<b>14</b>
Datei- und Internetspuren löschen .....	14
Tastaturaufzeichnung blocken .....	14
Weitere Überwachungen blocken .....	14
Warnen bei Autostart-Registryänderungen .....	14
<b>Teil V Bestell-Informationen</b>	<b>16</b>
Anmerkungen zur nicht registrierten Testversion .....	16
Freischaltcode bestellen .....	16
Freischalten zur Vollversion .....	16
<b>Index</b>	<b>17</b>

# Was kann der Security Task Manager?

**Teil**



## I. Was kann der Security Task Manager?

Der Security Task Manager zeigt Ihnen erweiterte Informationen zu Programmen und Prozessen, die auf dem Computer ausgeführt werden. Im Unterschied zum Windows Task-Manger sehen Sie zusätzlich zu jedem Prozess:

- ▶ Dateiname und Verzeichnispfad
- ▶ sicherheitsrelevante Bewertung
- ▶ Beschreibung
- ▶ Startzeit
- ▶ Diagramm der CPU-Auslastung
- ▶ Programmicon
- ▶ enthaltene versteckte Funktionen  
(z.B. Tastaturaufzeichnung, Browser-Überwachung, Manipulation)
- ▶ Prozess-Typ  
(sichtbares Fenster, DLL, in Taskleiste verankert, IE-Plugin, Dienst)

Der Security Task Manager erkennt auch Virtuelle Treiber, Dienste, BHO's oder Prozesse, die sich vor dem Windows Task-Manager verstecken.

Name	Bewertung	CPU	Datei	Typ	Hersteller: Produkt
XPCSpy, Monitor all activities of PC	100	0 %	C:\Programme\XPCSpy\XPCSpy.exe	Programm	X Software Studio :
Stub Loader Module	72		C:\WINNT\System32\amcis2.dll	Internet	: Stub Module
RmtAgent Module	67		C:\Programme\Shareware\EZ P... \RmtAgent.dll	Internet	Holoview International Co. : EZ Popu...
Google IE Client Toolbar	67		c:\winnt\... \googletoolbar_en_2.0.95-deleon.dll	Internet	Google Inc. : Google Toolbar for IE
IPC Server	42	0 %	C:\WINNT\System32\smipcsv.exe	Programm	Radiate : IPC Server
ZipToA	42	0 %	C:\WINNT\System32\ZipToA.exe	Programm	Iomega Corporation : Iomega ATAPI ...
FileBox eXtender	42	0 %	C:\Programme\Shareware\FileBX\FileBX.exe	Taskicon	Hyperionics : FileBox eXtender
ElbyCDIO Filter Driver	41		C:\WINNT\System32\Drivers\ElbyCDFL.sys	Treiber	Elaborate Bytes AG : CloneCD
ELSA ERAZOR III driver	41		C:\WINNT\System32\DRIVERS\eez3m.sys	Treiber	ELSA AG (Aachen, Germany) : ELSA...
Eumex 604PC HomeNet	41		C:\WINNT\System32\Drivers\CAPI20.SYS	Treiber	DeTeWe Berlin : CAPI Treiber
Telekom CapiPort	41		C:\WINNT\System32\drivers\detewecp.sys	Treiber	DeTeWe Berlin : DeTeWe ISDN CA...
Telekom Eumex 704PC ...	41		C:\WINNT\System32\DRIVERS\dtwmnic5.sys	Treiber	DeTeWe Berlin : NDIS NIC Miniport ...
Telekom Eumex x04PC [...]	41		C:\WINNT\System32\Drivers\ulisa.sys	Dienst	DeTeWe Berlin : USB Treiber
TrueVector Device Driver	32		C:\WINNT\System32\vsdatant.sys	Treiber	Zone Labs, Inc : TrueVector Device ...
eMule	22	0 %	C:\Programme\Shareware\emule\emule.exe	Taskicon	http://www.emule-project.net : eMule
EZ Popup Blocker		2 %	C:\Programme\Shareware... \PopupBlocker.exe	Taskicon	Holoview : EZ Popup Blocker Applic...
RapidKey - Autotext+Ma...		0 %	C:\Programme\Shareware... \RAPIDKEY.EXE	Taskicon	Neuber GbR : Neuber GbR / RapidK...
SETI@home		95 %	C:\Programme\Shareware... \SETI@home.exe	Taskicon	University of California, Berkeley : SE...
Microsoft IntelliPoint Fe...			C:\WINNT\System32\DRIVERS\IPFilter.sys	Treiber	Microsoft Corporation : Microsoft Poin...
Security Task Manager		2 %	C:\Programme\Borland\Delphi7... \taskman.exe	Programm	Neuber GbR : Security Task Manager
Delphi-32 Development ...		0 %	C:\Programme\Borland\Delphi7... \delphi32.exe	Programm	Borland Software Corporation : Profe...
ZoneAlarm		0 %	C:\Programme\Shareware\Zo... \zonealarm.exe	Taskicon	Zone Labs, Inc : ZoneAlarm
Windows Explorer		1 %	C:\WINNT\Explorer.exe	Programm	Microsoft Corporation : Betriebssystem...

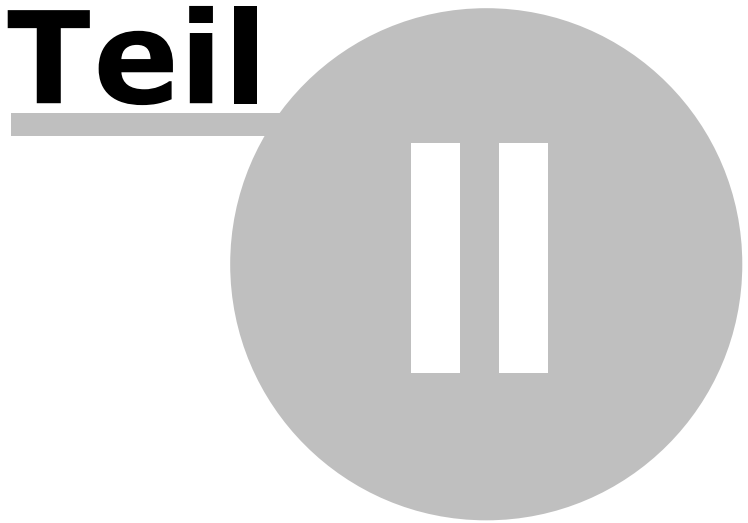
XPCSpy, Monitor all activities of PC		Eigenschaften	Bewertung	Enthaltene Texte
Hersteller	X Software Studio	Kann Tastatur Eingaben aufzeichnen	■■■■■■■■■■	ShellExecuteA
Beschreibung	Xpcspy	Nicht sichtbares Fenster	■■■■■■■■■■	VarNot
Typ	Programm, unsichtbar	Keine Windows System Datei	■■■■■■■■■■	OleDraw
Start	13:05:18, beim Windows Start	Starten beim Windows Start: Machine\Run	■■■■■■■■■■	SetKeyboardHook
Datei	C:\Programme\XPCSpy\XPCSpy.exe	Fehlende Beschreibung des Programms	■■■■■■■■■■	GetNetworkParams
Kommentar	Überwachungsprogramm	Funktionen: nicht ermittelbar	■■■■■■■■■■	GetOpenFileNameA
				ImageList_Add
		<b>Urteil: potentiell gefährlich</b>		GetAce

Security Task Manager analysiert objektiv die in den Prozessen enthaltenden Eigenschaften und kann daraus Rückschlüsse auf deren Gefährlichkeit ziehen.

Einige systemnahe Tools und Treiber haben Eigenschaften, die bei böswilliger Absicht, den Computer auch schaden könnten oder die zur Überwachung der Benutzeraktivitäten dienen könnten. Typisches Beispiels hierfür sind Firewalls und Antivirus-Wächter. Diese arbeiten (wie auch Trojaner) verdeckt im Hintergrund, überwachen Ihre Aktivitäten (z.B. Dateizugriffe, Netzwerk Traffic, etc). Wenn bei diesen Prozessen dann noch Dateibeschreibung oder digitale Signatur (von Microsoft heutzutage verlangt) fehlen, dann sind dies Indizien wie bei Schädlingen. Hier müssen Sie beurteilen, ob die Prozesse vertrauenswürdig sind.

# Arbeiten mit dem Security Task Manager

**Teil**



## II. Arbeiten mit dem Security Task Manager




### Überblick

Security Task Manager zeigt Ihnen alle aktiven Prozesse auf Ihrem PC an. Anhand der Bewertung können Sie abschätzen, welche sicherheitsrelevanten Funktionen die Prozesse enthalten.


Die aufgelisteten Prozesse können nach folgenden Kriterien sortiert werden. Im Menü **Ansicht** können Sie wählen, welche Kriterien als Spalten in der Prozess-Liste angezeigt werden.

- Name
- [Bewertung](#)
- Prozess ID (PID)
- CPU
- Speicher (RAM)
- Aktive Laufzeit
- Datei
- [Typ](#)
- Start
- Titel und Beschreibung
- Hersteller und Produkt

Klicken Sie auf einen Prozess, um genauere Informationen über diesen zu erhalten oder um ihn zu stoppen. Sie können:

-  [Eigenschaften ansehen](#)
-  [Prozess beenden](#)
-  [Prozess unter Quarantäne stellen](#)

#### **Anmerkung**




- Windows-Systemprozesse werden standardmäßig nicht angezeigt. Klicken Sie auf den Button  **System Prozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.
- Wenn Sie mit einem Standard Benutzerkonto bei Windows angemeldet sind, sehen Sie eventuell bei einigen Windows-interne Prozesse: <taskeng.exe - Services - Zugriff verweigert> Bitte starten Sie in diesem Fall den *Security Task Manager* als Administrator, indem Sie auf dem *Security Task Manager*-Icon mit der rechten Maustaste klicken und dann **Als Administrator ausführen** anklicken.

### Anzeigen der Prozess Eigenschaften


Klicken Sie auf einen Prozess, um genaue Angaben zu diesen Prozess zu sehen. Folgende Eigenschaften werden hierbei angezeigt:

- Name
- [Bewertung](#)
- Hersteller
- Beschreibung
- [Typ](#)
- Start
- Datei
- [Kommentar](#)

So erhalten Sie noch mehr Informationen oder stoppen den Prozess:

-  [Informationen aus dem Web zu diesem Prozess](#)
-  [Prozess beenden](#)
-  [Prozess unter Quarantäne stellen](#)

## Anzeigen von weiteren Eigenschaften (Google Suche)


- 1 Klicken Sie auf den Prozess, über Sie mehr möchten.
- 2 Klicken Sie auf  **Google**.

Es wird nun eine Informationsseite auf [www.neuber.com/taskmanager](http://www.neuber.com/taskmanager) angezeigt, wo Sie Ihre Meinung zu dieser Software/Treiber schreiben können oder Kommentare anderer User lesen können. Von dieser Seite aus können Sie bei [Google.com](http://Google.com) nach weiteren Informationen über diesen Prozess suchen.

### **Anmerkung**

- Ihr Internet-Browser übermittelt Informationen (z.B. Betriebssystem, eingestellte Sprache). Weder das Programm Security Task Manager noch eine seiner Komponenten stellt eine Verbindung zum Internet her.
- [Google.com](http://Google.com) ist eine der meist genutztesten Suchmaschinen im Internet, die sehr gute Resultate liefert.

## Beenden eines Prozesses

- 1 Klicken Sie auf den Prozess, welchen Sie beenden möchten.
- 2 Klicken Sie auf  **Entfernen**.
- 3 Wählen Sie nun eine der folgenden Optionen:
  - Prozess beenden
  - Datei in Quarantäne-Ordner verschieben
  - Deinstallieren


### **Anmerkung**

- Das Beenden eines Prozesses kann zu Instabilitäten und Datenverlust führen. Programme oder auch Windows können abstürzen. Bitte sichern Sie geöffnete Dokumente.
- Sie können einen **Wiederherstellungspunkt setzen**, um bei Instabilitäten Ihr System wiederherstellen zu können.
- Für alle Aktionen in diesem Dialog benötigen Sie Administrator-Rechte. Um Security Task Manager mit Administrator-Rechten zu starten, klicken Sie bitte mit der rechten Maustaste auf die Verknüpfung und dann auf **Ausführen als...**

## Quarantäne-Ordner

Der Quarantäne-Ordner funktioniert wie ein Papierkorb für beendete Prozesse. Wenn Sie eine [Datei in den Quarantäne-Ordner verschieben](#), so wird die Datei in einen abgeschotteten Ordner verschoben und umbenannt. Auch AutoStart-Einträge in der Registry werden gelöscht. Damit ist die Datei nicht mehr ausführbar. Da Security Task Manager alle seine Aktivitäten speichert, ist eine Wiederherstellung des Prozesses jederzeit möglich.

### **So stellen Sie Prozesse wieder her**

- 1 Klicken Sie in der Symbolleiste auf  **Quarantäne**.
- 2 Klicken Sie im Quarantäne-Ordner auf den gewünschten Prozess.
- 3 Klicken Sie auf den Button **Wiederherstellen**.


### **Anmerkung**

- Sie können im  [Entfernen](#) Dialog einen **Wiederherstellungspunkt setzen**, um bei Instabilitäten Ihr System wiederherstellen zu können.

## Drucken der Prozess Liste

- 1 Klicken Sie im Menü Datei auf **Drucken**.
- 2 Wählen Sie den Drucker und eventuelle Eigenschaften (z.B. beidseitiger Druck).


### Anmerkung

- Windows-Systemprozesse werden standardmäßig nicht angezeigt und demzufolge nicht ausgedruckt. Klicken Sie auf den Button  **System Prozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen und drucken zu können.

## Exportieren der Prozess-Liste

- 1 Klicken Sie im Menü Datei auf **Exportieren nach**.
- 2 Wählen Sie als Dateityp:
  - Website (\*.html)
  - Text file (\*.txt)

### Anmerkung

- Windows-Systemprozesse werden standardmäßig nicht angezeigt und demzufolge nicht exportiert. Klicken Sie auf den Button  **System Prozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen und speichern zu können.
- Speichern Sie die Prozess Liste von Zeit zu Zeit, um neue Prozesse auffindig zu machen. Eine gespeicherte Prozess Liste kann auch als Beweissicherung dienen.

## Kommentar und eigene Bewertung zu einem Prozess

Sie können zu jedem Prozess eine persönliche Anmerkung schreiben, die dann bei den [Prozess-Details](#) angezeigt wird. Weiterhin können Sie eine eigene Risiko-Bewertung abgeben, die bei der Security Task Manager Bewertung mit einfließt.

### So schreiben Sie einen Kommentar

- 1 Klicken Sie mit der rechten Maustaste auf den gewünschten Prozess.
- 2 Klicken Sie im Kontextmenü auf **Kommentar...**
- 3 Geben Sie nun Ihre Anmerkung und eventuelle eigene Risiko Bewertung ein.

## Überprüfen von Änderungen an Hosts Datei

Die Windows **hosts** Datei befindet sich standardmäßig im Ordner `c:\Windows\system32\drivers\etc`. Diese Textdatei enthält Zuordnungen von IP-Adressen zu Web-Adressen (z.B. `www.file.net`). Wenn die hosts Datei ohne Ihr Wissen geändert wurde, besteht der Verdacht, dass ein Computerschädling wichtige Webseiten (z.B. von Banken, Antivirenhersteller) auf eine gefälschte Webseite umleitet. Die hosts Datei kann mit dem Windows Editor bearbeitet werden. Um eine Umleitung zu deaktivieren, geben Sie einfach das Zeichen `#` vor der IP-Adresse ein oder löschen die Zeile.

### Anmerkung

- Die *hosts* Datei ersetzt DNS (Domain Name Service). Die *lmhosts* Datei im gleichen Ordner ersetzt WINS, ist also für die Zuordnung von IP-Adressen zu Computer in Ihrem LAN Netzwerk wichtig.

## Ändern der Sprache

Security Task Manager erkennt automatisch die verwendete Sprache (Englisch, Deutsch, ...). Um die Sprache zu ändern, machen Sie bitte folgendes:

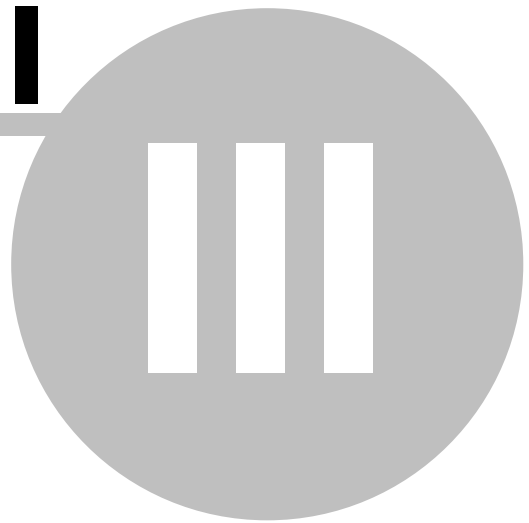
1. Klicken Sie im Menü **Ansicht** auf **Sprache** ▶.
2. Klicken Sie auf die gewünschte Sprache.

### **Anmerkung**

- Sie können Security Task Manager ganz einfach in eine weitere Sprache übersetzen. Hierzu muß nur die die Textdatei lgs\_deutsch.txt im Programm-Verzeichnis übersetzt und an [info@neuber.com](mailto:info@neuber.com) geschickt werden. Als Dankeschön für Ihre Übersetzung erhalten Sie eine kostenlose Vollversion.
- To read how to change the language please click [here](#).

# Grundlagen

**Teil**



### III. Grundlagen

#### Risiko-Bewertung der Prozesse

Security Task Manager bewertet das sicherheitsrelevante Risiko eines Prozesses nach objektiven Kriterien. Hierzu wird untersucht, ob der Prozess kritische Funktionsaufrufe oder verdächtige Eigenschaften enthält. Je nach potentieller Gefährlichkeit dieser Funktionen und Eigenschaften werden Punkte vergeben. Die Summe ergibt dann die Gesamt-Wertung (0 bis maximal 100 Punkte).

Eigenschaften	Bewertung
Nicht sichtbares Fenster	■ ■ ■ ■ ■ ■ ■ ■
Sendet an WindowsXP auf Port 0	■ ■ ■ ■ ■ ■ ■ ■
Keine Windows System Datei	■ ■ ■ ■ ■ ■ ■ ■
Starten beim Windows Start: Machin...	■ ■ ■ ■ ■ ■ ■ ■
Funktionen: Internet, Überwachen, V...	■ ■ ■ ■ ■ ■ ■ ■

**Urteil: potentiell gefährlich**

Security Task Manager untersucht die Prozesse nach folgenden Funktionalitäten (Sortierung nach Gefährlichkeit):

- Kann Tastatur Eingaben aufzeichnen
- Getarnter Prozess ist unsichtbar
- Datei ist nicht sichtbar
- Tastatur-Treiber, könnte Eingaben aufzeichnen
- Kann andere Programme manipulieren
- Kann Internet Browser überwachen
- Startet beim Start anderer Programme
- Lauscht auf Port <Nr>
- Sendet an <Computername> auf Port <Nr>
- Unbekanntes Programm lauscht und sendet
- Überwachen von Programmstarts
- Nicht sichtbares Fenster
- Starten beim Windows Start
- Keine ausführlich Beschreibung vorhanden
- Unbekannte Datei im Windows Ordner
- Keine Windows System Datei
- Fehlende Beschreibung des Programms
- Funktionen: Internet, Überwachen, Eingabe aufzeichnen, Verstecken, Manipulieren
- Funktionen: nicht ermittelbar
- Unbekannter Hersteller

Vertrauenswürdige Eigenschaften (verbessern die Risiko-Bewertung):

- Microsoft signierte Datei
- Verisign signierte Datei
- Gehört zu <Software Produkt> von <Hersteller>
- Zertifiziert von <Hersteller>
- [Eigener Kommentar](#)

Klicken Sie auf einen obigen Typ, um mehr darüber zu erfahren.

#### Anmerkung

- Hoch bewertete Programme müssen nicht zwingend gefährlich sein. Sie besitzen eventuell nur für Spyware typische Funktionen.
- Windows-Systemprozesse werden standardmäßig nicht angezeigt. Klicken Sie auf den Button **System Prozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.

## Prozess Typen

Security Task Manager unterscheidet folgende Arten von Prozessen. Im Menü **Ansicht** können Sie einstellen, dass der **Typ** als Spalte mit angezeigt wird. Sie können jedoch auch am Icon erkennen, um welchen Typ es sich handelt.


### Software

- Programm
- Taskbar Icon

### DLL Dateien

- DLL
- ShellExecute

### Internet-PlugIns


 Browser Helpers Objects

### Treiber und Dienste

 Gerätetreiber

 Dateitreiber

 Dienst (eigener Prozess)


 Dienst (eigener Prozess mit Desktop-Interaktion)

 Dienst (beteiligter Prozess)

 Dienst (beteiligter Prozess mit Desktop-Interaktion)

Klicken Sie auf einen obigen Typ, um mehr darüber zu erfahren.

### Anmerkung

- Windows-Systemprozesse werden standardmäßig nicht angezeigt. Klicken Sie auf den Button  **System Prozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.

## Wie Sie das Security Task Manager Team erreichen

Technischer Kontakt:

Anschrift: A. & M. Neuber Software GmbH  
PF 11 05 25  
D-06019 Halle  
Fax: (+49) 0700-11 777 000  
Internet:  
WWW: [www.neuber.com/taskmanager](http://www.neuber.com/taskmanager)  
email: [info@neuber.com](mailto:info@neuber.com)

An English version is available at <http://www.neuber.com/taskmanager>

## Deinstallieren

- 1 Klicken Sie auf Start-Einstellungen-Systemsteuerung.
- 2 Klicken Sie auf **Software**.
- 3 Klicken Sie auf den Button **Hinzufügen/Entfernen**, um Security Task Manager vollständig von Ihrem Computer zu löschen

### Anmerkung

- Sollte Security Task Manager nicht als Software mit aufgelistet sein, dann starten Sie bitte `uninstal.exe` im Security Task Manager-Verzeichnis.

# Schutz mit SpyProtector

**Teil**

---



**IV**

## IV. Schutz mit SpyProtector

### Datei- und Internetspuren löschen

Der SpyProtector bieten Ihnen folgende Werkzeuge, um sich vor Keyloggern, Spyware und Trojanern zu schützen:

#### **Datei- und Internetspuren löschen**

Hiermit können Sie Ihre Internet-Spuren (Cookies, Cache, Verlauf, eingetippte Webadressen) im InternetExplorer löschen. Weiterhin können Sie auch die Liste der zuletzt benutzten Programme (z.B. im Startmenü) und Dokumente (z.B. in Word, ACDSsee, PDF, WinZip, Mediaplayer) löschen.

#### ✓ **Tastaturaufzeichnung nicht erlauben**

Hiermit können die meisten Tastatur-Überwachungsprogramme (Keylogger) für die aktuelle Windows Sitzung unschädlich gemacht werden. Es wird die Umleitung aller Tastatureingaben über Fremdprogramme bis zum nächsten Windows-Start blockiert. So eine Tastatur-Umleitung wird programmieretechnisch per Hook realisiert. Selbst Tastatur-Utilities wie Macro- und Autotext-Programme verwenden solche unsauberen Hooks nicht.

#### ✓ **Andere Überwachungen nicht erlauben**

Hiermit können für die aktuelle Windows Sitzung Überwachungsprogramme unschädlich gemacht werden, die heimlich folgendes aufzeichnen:

##### ***Tastatureingaben (indirekt)***

Alle Windows internen Nachrichten, also auch Tastatureingaben werden überwacht.

##### ***Mausaktivitäten***

Alle Mausbewegungen und Mausklicks werden überwacht.

##### ***Makro***

Aufnehmen und Abspielen von Benutzeraktivitäten. Diese oft von Makroprogrammen verwendete Funktion ist für Keylogger unüblich, wäre jedoch theoretisch möglich.

##### ***Programmstart- und Ende***

Das Aufrufen und Schließen von Programmen wird protokolliert. Diese Funktion wird häufig von Lernprogrammen (CBT) zur Interaktion mit der zu erlernenden Software genutzt.

Achtung: Einige seriöse Programme (z.B. manche Macro-Programme) nutzen diese "unsauberen" Hook-Funktionen, mit denen Nachrichtenströme abgehört werden können. Sollte so ein Programm nicht mehr funktionieren, so deaktivieren Sie bitte die entsprechende Option/Funktion oder starten Ihren PC neu.

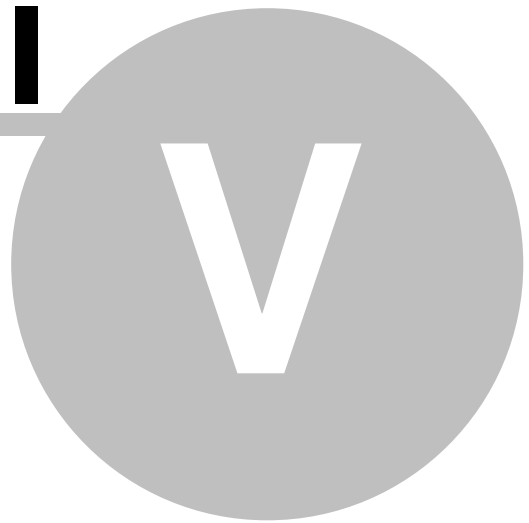
#### ✓ **Warnen bei Autostart-Registryänderung**

Sie erhalten eine Messagebox, wenn ein Programm versucht, sich als Autostart in der Windows Systemregistrierung einzutragen. Mit so einem Eintrag, der sichtbar oder unsichtbar sein kann, wird die Software bei jedem Windows-Start heimlich gestartet. Alle schädlichen Programme benötigen so einen Eintrag, um bei einem Rechner-Neustart aktiv zu sein!

# Bestell-Informationen

**Teil**

---



## V. Bestell-Informationen

### Anmerkungen zur nicht registrierten Testversion

**Security Task Manager** ist keine kostenlose Software, sondern wird als Shareware vertrieben. Sie dürfen die Shareware-Version 30 Tage testen. Gefällt Ihnen das Programm oder möchten Sie es auch weiterhin benutzen, so müssen Sie Security Task Manager für 29 EUR [registrieren](#).

Als registrierter Anwender erhalten Sie:




- das volle Nutzungsrecht für Security Task Manager
- umgehend Ihren Freischaltcode zum [Freischalten](#) dieser Version
- kostenlose Updatemöglichkeit auf alle 1.x Versionen
- die Software SpyProtector  
SpyProtector verhindert die Überwachung von Tastatureingaben, Mausebewegungen, Programmstarts und warnt bei Autostart-Registryänderungen
- kostenlose Problem- und Pannenhilfe
- keine Shareware-Hinweise und -Beschränkungen mehr

Klicken Sie im Menü **Hilfe** auf **Info...**, um zu erfahren, ob das Programm schon freigeschaltet und registriert ist.

### Freischaltcode bestellen

Sie erhalten Ihren Freischaltcode für 29 EUR beim Registrierservice ShareIt sofort per email, per Brief oder per Fax. Die Lizenzgebühr können Sie per Kreditkarte, Überweisung, Scheck oder Bargeld bezahlen.

Bestellen Sie ganz einfach

-  **im Internet:** [Online-Bestellformular](#)
-  **per Brief/Fax:** [Bestellformular zum Ausdrucken](#)
-  **per Telefon:** +49-221-31088-20 (ShareIt, Köln)  
Bestell-Nr.: 174510

#### **Anmerkung**

- Nutzen Sie die Vorteile der [Online-Bestellung](#)
  - Erhalt des Freischaltcodes per email sofort nach Zahlungseingang
  - sichere Online-Verbindung
- Fragen zur Registrierung beantwortet Ihnen: ShareIt/element 5 AG, Vogelsanger Str. 78, D-50823 Köln, Fax: +49-221-3108829, Telefon: +49-221-3108820, support@shareit.com
- Fragen zur Software beantwortet Ihnen das [Security Task Manager Team](#).

### Freischalten zur Vollversion

- 1 Klicken Sie im Menü **REGISTRIEREN** auf **Freischalten**.
- 2 Geben Sie nun die Registrierdaten genau so ein, wie Sie sie von uns erhalten haben.
- 3 Klicken Sie auf **Freischalten**.

#### **Anmerkung**

- Bei Fragen, wenden Sie sich bitte an [uns](#).
- Ihren [Freischaltcode erhalten](#) Sie innerhalb von 24 h.

# Index

## - A -

Anmerkung 8

## - B -

Beenden eines Prozesses 7  
Bestellen 16  
Bewertung 11  
BHO 12  
Browser Helpers Objects 12

## - D -

Deinstallation 12  
Details 6  
Dienst 12  
DLL 12  
Driver 12  
Drucken 8

## - E -

Eigenschaften eines Prozesses 6  
Exportieren nach... 8

## - F -

Freischaltcode  
Freischaltcode bestellen 16  
Freischalten der Shareware-Version 16  
Freischalten der Shareware-Version 16

## - G -

Google Suche 7

## - H -

hosts Datei 8

## - I -

Impressum 12  
Internet  
Info über Prozess suchen 7

Produkt Homepage 12  
Prozess Typ 12  
Spuren löschen 14

## - K -

Kommentar 8  
Konzept von Security Task Manager 6

## - M -

Menüsprache 9

## - O -

Ordner 7

## - P -

Preis der Vollversion 16  
Programm 12  
Prozess  
Arten 12  
beenden 7  
Bewertung 11  
drucken 8  
Eigenschaften 6  
Kommentar 8

## - Q -

Quarantäne 7

## - R -

Rating 11  
Registrierung  
Freischaltcode bestellen 16  
Freischalten der Shareware-Version 16  
Registry Warner 14  
Risiko 11

## - S -

Security Task Manager  
Anmerkungen zur nicht registrierten  
Testversion 16  
deinstallieren 12  
Info... 12  
So funktioniert 6  
Was kann Security Task Manager 4

Service 12

Shareware

Freischaltcode bestellen 16

Freischalten mit Freischaltcode 16

Speichern

Drucken 8

Exportieren 8

Sprache

ändern 9

SpyProtector 14

## - T -

Task 6

Taskbar Icon 12

Tastaturaufzeichnung verhindern 14

Treiber 12

Typ 12

## - U -

Über Security Task Manager 12

Überblick 4

Überwachung verhindern 14

## - W -

Web Informationen 7