Security Task Manager

für Windows XP, 2000, NT, ME, 98

Security Task Manager zeigt alle Informatione zu Programmen und Prozessen

Inhalt

Was kann Security Task Manager?.....3

So funktioniert Security Task Manager 3

Prozess Typen.....4

Risiko-Bewertung der Prozesse 5

So sehen Sie Details eines Prozesses 7

So erfahren Sie mehr über einen Prozess 7

So beenden Sie einen Prozess.....8

So funktioniert der Quarantäne-Ordner 8

So exportieren Sie die Prozess Liste.....9

So drucken Sie die Prozess Liste 9

So schreiben Sie einen Kommentar zu einem Prozess 9

So schützen Sie sich mit SpyProtector.....10

So ändern Sie die Sprache.....11

So fügen Sie eine neue Sprachdatei hinzu 11

So erreichen Sie das Security Task Manager Team 11

So deinstallieren Sie Security Task Manager 11

Anmerkungen zur nicht registrierten Testversion.....12

So schalten Sie die Shareware-Version frei 12

Was kann 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, Programmicon
- Diagramm der CPU-Auslastung
- Prozess-Typ
- enthaltene versteckte Funktionen
  (z.B. Tastaturaufzeichnung, Browser-Überwachung, Manipulation)

Die Software SpyProtector verhindert die Aufzeichnung von Tastatureingaben, Mausbewegungen, Programmstarts und warnt bei Autostart-Registryänderungen.

So funktioniert der Security Task Manager

Die software 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** wählen Sie, welche Kriterien als Spalten in der Prozess-Liste angezeigt werden.

- Name
  Zeigt den Namen der Software oder des Treibers an.
- Bewertung
  Zeigt eine sicherheitsrelevante Beurteilung des Prozesses. Je länger der Bewertungsbalken, desto gefährlichere Funktionen enthält der Prozess. Hoch bewertete Programme müssen nicht zwingend gefährlich sein. Sie besitzen eventuell nur für Spyware typische Funktionen. Bitte klicken Sie auf einen Prozess, um genauere Details zu erfahren und die Vertrauenwürdigkeit der Software abzuschätzen.
- CPU
  Zeigt die Inanspruchnahme des Prozessors. Aktive Programme benötigen mehr Prozessorleistung als inaktive Prozesse. Wenn Sie die Spalte verbreitern, sehen Sie den zeitlichen Verlauf der CPU-Belastung der Prozesse. Hierzu ziehen Sie einfach den Spaltenkopf breiter.
- Speicher
  Zeigt den Arbeitsspeicher-Bedarf eines Prozesses.
- Datei
  Zeigt den Pfad und den Namen der Datei.
- Typ
  Zeigt ob es sich um ein Programm, ein in der Taskleiste verankertes Programm, BHO, Treiber oder Dienst handelt.
- Titel und Beschreibung
  Zeigt den Titel und die in der Datei enthaltene Datei-Beschreibung. Bei einem sichtbarem Fenster entspricht der Titel dem Text in der Titelleiste.
- Hersteller und Produkt
  Zeigt Name des Herstellers und die in der Datei gespeicherte Produktbeschreibung.

Für weitere Informationen klicken Sie auf den Prozess. Sie können:

Eigenschaften ansehen

Prozess beenden

Prozess unter Quarantäne stellen

Anmerkung

- Klicken Sie auf den Button **Systemprozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem. Windows-Systemprozesse werden standardmäßig nicht angezeigt.
- Ein Prozess bezeichnet ein Programm, Treiber, Dienst oder PlugIn - also jeden ausführbaren Code, der im Arbeitsspeicher Ihres Computers aktiv ist.

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
  Der als Programm bezeichnete Prozess kann sichtbar (als normales Windows-Fenster) oder unsichtbar sein.
- Taskbar Icon
  Programm, dessen Icon in der Taskleiste (links neben der Uhrzeit) verankert ist. Klicken Sie mit der rechten Maustaste auf das Icon in der Taskleiste, um ein Kontextmenü zu öffnen und mehr über das Programm zu erfahren.

DLL Dateien

- DLL
  Eine Dynamic Link Library (DLL) enthält ausführbaren Programmcode. In einer DLL-Datei sind im Standardfall selten genutzte Funktionen ausgelagert, die nur bei Bedarf vom Hauptprogramm ausgeführt werden. Dadurch benötigt das Hauptprogramm weniger Arbeitsspeicher.
- SheelExecute
  Die Datei wurde über den Befehl ShellExecute in der Windows Systemregistrierung (Konfigurationsdatei) per Hook gestartet. ShellExecute startet einen Prozess (meistens eine DLL) sobald ein beliebiges Windows-Programm gestartet wurde. Dieser Prozess sollte genau untersucht werden.

Internet-PlugIns


Browser Helpers Objects
Browser Helper Objects klinken sich in den InternetExplorer ein. Meistens handelt es sich um erwünschte Download-Manager oder andere kleine Tools. Allerdings können BHO's auch Ihre Surfverhalten überwachen. Um BHO's abzuschalten, klicken Sie im Internet Explorer im Menü **Extras** auf **Internetoptionen** und deaktivieren im Reiter **Erweitert** die Option **Browsererweiterungen von Drittanbietern aktivieren**.

Treiber und Dienste

Treiber und Dienste führen Systemfunktionen auf unterer Hardware-Ebene zur Unterstützung anderer Programme aus. (nur in der Vollversion)


Gerätetreiber
Gerätetreiber zum Betrieb von Hardwarekomponenten. Das können Treiber für Grafikkarte und Scanner sein. Aber auch Programme, die nicht von einem User oder Programm beendet werden sollen (z.B. Firewall, AntiVirus-Modul).


Dateitreiber
Treiber für das auf Windows NT basierende Dateisystem.


Dienst (eigener Prozess)
Ein System- oder Hardwarenaher Prozess zur Unterstützung anderer Programme. Der Dienst wird als eigener Prozess ausgeführt.


Dienst (eigener Prozess mit Desktop-Interaktion)
Ein System- oder Hardwarenaher Prozess zur Unterstützung anderer Programme. Der Dienst wird als eigener Prozess ausgeführt, der mit dem Desktop interagieren kann (z.B. Firewall, AntiVirus-Modul).


Dienst (beteiligter Prozess)
Der Dienst teilt sich mit anderen Diensten einen Prozess.


Dienst (betreiligter Prozess mit Desktop-Interaktion)
Der Dienst teilt sich mit anderen Diensten einen Prozess. Der Prozess kann mit dem Desktop interagieren.

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).

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

- Kann Tastatur Eingaben aufzeichnen
  Der Prozess überwacht jede Tastatureingabe. Per Hook werden die Eingaben mitgelesen. Sauber programmierte, seriöse Programme nutzen diese Hook-Funktion nicht.
- Datei ist nicht sichtbar
  Die Datei versteckt sich vor dem Windows Explorer. Bitte nicht verwechseln mit dem harmlosen Dateiattribut "versteckt".
- Tastatur-Treiber, könnte Eingaben aufzeichnen
  Es handelt sich um einen Tastatur-Treiber, der jede Eingabe mitlesen kann.
- Kann andere Programme manipulieren
  Der Prozess kann sich in anderen Programmen einklinken und dort etwas zu verändern. Hierzu wird ein Hook gesetzt, der z.B. allen Programmen eine gefälschte Dateiliste vortäuschen könnte (dir-Befehl ändern). Das Programm wäre dann für andere Programme (AntiVirus) unsichtbar.
- Kann Internet Browser überwachen
  Browser Helper Objects klinken sich in den InternetExplorer ein. Meistens handelt es sich um erwünschte Download-Manager oder andere kleine Tools. Allerdings können BHO's auch Ihre Surfverhalten überwachen. Um BHO's abzuschalten, klicken Sie im Internet Explorer im Menü **Extras** auf **Internetoptionen** und deaktivieren im Reiter **Erweitert** die Option **Browsererweiterungen von Drittanbietern aktivieren**.
- Startet beim Start anderer Programme
  Die Datei wurde über den Befehl ShellExecute in der Windows Systemregistrierung (Konfigurationsdatei) per Hook gestartet. ShellExecute startet einen Prozess (meistens eine DLL) sobald ein beliebiges Windows-Programm gestartet wurde. Dieser Prozess sollte genau untersucht werden.
- Lauscht auf Port *<Nr>*
  Der Prozess kann über diese offene Stelle Informationen empfangen. Hacker nutzen solche Schwachstellen aus, um in einen fremden Rechner einzudringen und die Kontrolle über diesen zu erlangen. Mit einer guten Firewall können solche Attacken verhindert werden.
- Sendet an *<Computername>* auf Port *<Nr>*
  Der Prozess hat eine Verbindung zum angegebenen Computer bzw. IP-Adresse hergestellt und kann darüber beliebige Informationen senden. Mit einer guten Firewall können solche Verbindungen geblockt werden.
- Unbekanntes Programm lauscht oder sendet
  Es wurde ein Port geöffnet, um Informationen von außen zu empfangen oder dorthin zu senden. Bitte stellen Sie fest, um welches Programm es sich handelt. Mit einer guten Firewall kann die Verbindungen blockiert werden.

Fortsetzung auf der nächsten Seite

- Überwachen von Programmstarts
  Der Prozess zeichnet auf, wann welche Programme aufgerufen und beendet werden.
- Nicht sichtbares Fenster
  Das Programm hat kein sichtbares Windows Fenster und läuft im Hintergrund. Im günstigsten Fall handelt es sich z.B. um Gerätetreiber.
- Starten beim Windows Start
  Das Programm wird bei jedem Windows-Start aufgerufen. Hierzu hat sich das Programm in einen Autostart-Schlüssel inder Windows Systemregistrierung eingetragen.
- Keine ausführlich Beschreibung vorhanden
  Einige wichtige Standard-Beschreibungen in der Datei wurden nicht gefunden. Standardmäßig enthält jede Datei intern Felder für Beschreibungen.
- Keine Windows System Datei
  Die Datei gehört nicht zum Windows Betriebssystem. Windows Systemdateien werden von Windows besonders überprüft und geschützt.
- Fehlende Beschreibung des Programms
  Es wurden keine Beschreibungen in der Datei gefunden. Standardmäßig enthält jede Datei intern einige Felder für Beschreibungen.
- Funktionen: Internet, Überwachen, Eingabe aufzeichnen, Verstecken, Manipulieren
  Die Datei enthält Funktionsaufrufe mit den angegebenen Eigenschaften. Da jedoch nicht gesagt werden kann, ob und wie diese zum Einsatz kommen, wird dieses Kriterium nicht stark gewichtet.
- Funktionen: nicht ermittelbar
  In der Datei wurden keine gefährlichen Funktionsaufrufe gefunden. Diese könnten jedoch versteckt integriert sein.
- Unbekannter Hersteller
  Der Hersteller ist nicht ermittelbar. Standardmäßig enthält jede Datei intern Felder zur Angabe des Softwareherstellers.

Vertrauenswürdige Eigenschaften (verbessern die Risiko-Bewertung):

- Microsoft signierte Datei
  Diese Datei wurde von Microsoft signiert. Sie können dieser Datei vertrauen, so wie Sie auch Microsoft vertrauen.
- Verisign signierte Datei
  Diese Datei wurde von VeriSign signiert. Sie können dieser Datei vertrauen, so wie Sie auch VeriSign vertrauen.
- Zertifiziert von <*Zertifizierungsstelle*> für Firma <*Hersteller*>
  Diese Datei wurde von einer Zertifizierungsstelle signiert. Sie können dieser Datei vertrauen, so wie Sie auch der Zertifizierungsstelle und dem Softwarehersteller vertrauen.
- Eigener Kommentar
  Im eigenen Kommentar können Sie Ihre eigene Bewertung abgeben und so das Risiko Rating beeinflußen.

Anmerkung

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

So sehen Sie Details eines Prozesses

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

- Name
  Zeigt den Namen der Software oder des Treibers an.
- Bewertung
  Zeigt eine sicherheitsrelevante Beurteilung des Prozesses. Je länger der Bewertungsbalken, desto gefährlichere Funktionen enthält der Prozess. Hoch bewertete Programme müssen nicht zwingend gefährlich sein. Sie besitzen eventuell nur für Spyware typische Funktionen. Bitte klicken Sie auf einen Prozess, um genauere Details zu erfahren und die Vertrauenwürdigkeit der Software abzuschätzen.
- Datei
  Zeigt den Pfad und den Namen der Datei.
- Typ
  Zeigt ob es sich um ein Programm, ein in der Taskleiste verankertes Programm, BHO, Treiber oder Dienst handelt.
- Titel und Beschreibung
  Zeigt den Titel und die in der Datei enthaltene Datei-Beschreibung. Bei einem sichtbarem Fenster entspricht der Titel dem Text in der Titelleiste.
- Hersteller und Produkt
  Zeigt den Namen des Herstellers und die in der Datei gespeicherte Produktbeschreibung.

Anmerkung

- Klicken Sie auf den Button **Systemprozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Windows-Systemprozesse werden standardmäßig nicht angezeigt. Diese Prozesse gehören laut Microsoft zum Betriebssystem.
- Im Menü **Ansicht** können Sie wählen, welche Eigenschaften als Spalten in der Prozess-Liste angezeigt werden.

So erfahren Sie mehr über einen Prozess

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 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 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 ist eine der meist genutztesten Suchmaschinen im Internet, die sehr gute Resultate liefert.

So beenden Sie einen Prozess

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
  Der Prozess wird aus dem Arbeitsspeicher entfernt. Sollte der Prozess in der Registry (Windows-Konfigurationsdatenbank) als AutoStart eingetragen sein, so ist er jedoch beim nächsten Windows-Start wieder aktiv.
- Datei in Quarantäne-Ordner verschieben
  Auch hier wird der Prozess aus dem Arbeitsspeicher entfernt. Zusätzlich werden die entsprechende Datei in den Quarantäne-Ordner verschoben und AutoStart-Einträge in der Registry gelöscht. Da Datei und Registry-Einträge gesichert werden, ist eine Wiederherstellung des Prozesses möglich.

Anmerkung

- Das Beenden eine Prozesses kann zu Instabilitäten und Datenverlust führen. Programme oder auch Windows können abstürzen. Bitte sichern Sie geöffnete Dokumente.

So funktioniert der 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**.

So exportieren Sie die Prozess Liste

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

Anmerkung

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

So drucken Sie die Prozess Liste

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

Anmerkung

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

Schreiben Sie einen Kommentar zu einem Prozess

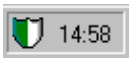
Sie können zu jedem Prozess eine persönliche Anmerkung schreiben, die dann bei den Prozess-Details angezeigt wird. Weiterhin können Sie eine eigene Risiko-Bewertung abgeben, die bei der Security Task Manager Bewertung mit einfließt.

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.

So schützen Sie sich mit SpyProtector

Um den SpyProtector zu starten, klicken Sie auf das Icon in der Task-Leiste.



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 benutzen Programme (z.B. im Startmenü) und Dokumente (z.B. in Word, ACDSee, 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 programmiertechnisch 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 aktivieren 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!

So ändern Sie die 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 geschickt werden. Als Dankeschön für Ihre Übersetzung erhalten Sie eine kostenlose Vollversion.

So fügen Sie eine neue Sprachdatei hinzu

Sie erhalten weitere Sprachdateien im Internet unter www.neuber.com/taskmanager/deutsch.

1. Geben Sie in Ihrem Internet-Browser www.neuber.com/taskmanager/deutsch ein.
2. Hier sehen Sie, welche Sprachen in der aktuellen Version enthalten sind.
3. Kopieren Sie die neuste Version einfach in das existierende Verzeichnis von Security Task Manager z.B. c:\Programme\Security Task Manager
4. Starten Sie nun Security Task Manager und ändern Sie die Sprache.

Anmerkung

- Die Sprachdateien lgs_deutsch.txt und lgs_english.txt sind standardmäßig schon enthalten.

So erreichen Sie das Security Task Manager Team

Technischer Kontakt:

Anschrift: Alexander und Matthias Neuber GbR
PF 11 05 25
D-06019 Halle
Fax: (+49) 0700-11 777 000
Internet:
WWW: www.neuber.com/taskmanager
email: info@neuber.com

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

So deinstallieren Sie Security Task Manager

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 Ihren Computer zu löschen

Anmerkung

- Alternativ starten Sie bitte uninstal.exe im Security Task Manager-Verzeichnis.

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 ein Leben lang
- die Software SpyProtector
  SpyProtector verhindert die Überwachung von Tastatureingaben, Mausbewegungen, 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.

So schalten Sie die Shareware-Version frei

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

- Leerzeichen, Enterzeichen, Kommas, Groß- und Kleinschreibung im Namen bleiben unbeachtet
  Martin JR. entspricht Martinjr