Klicken Sie auf **Hilfethemen**, um zur Liste der Hilfethemen zurückzukehren.

Entfernen von Prozessen: Wenn dies nicht funktioniert im abgesicherten Modus F8, sonst DOS booten
vgl Popup #Typ

Security Task Manager

Security Task Manager zeigt Ihnen **alle** Informationen zu Programmen und Prozessen, die auf dem Computer ausgeführt werden. Als Prozess Viewer findet Security Task Manager auch Software, die sich vor dem Windows Task-Manager verstecken.

Weitere Informationen

Vielen Dank, daß Sie Security Task Manager testen. Bitte lassen Sie sich registrieren, wenn Ihnen das Programm gefällt.

Vielen Dank, daß Sie Security Task Manager getestet haben. Die Testzeit des Programms von 30 Tagen ist nun abgelaufen. Bitte lassen Sie sich jetzt registrieren, wenn Sie das Programm auch weiterhin benutzen möchten.

Security Task Manager

Sie haben die Shareware Version von Security Task Manager mehr als 30 Tage getestet. Die Testzeit ist nun abgelaufen. Bitte registrieren Sie sich noch heute für nur 29 Euro.

Für mehr Informationen klicken Sie hier 

Sie arbeiten mit der Security Task Manager Testversion

Die Testversion zeigt Ihnen alle laufenden Prozesse.
Die Vollversion analysiert zusätzlich Dienste und Treiber auf Ihren PC.

{button Wie kaufe ich die Vollversion,JI(`taskman_de.hlp',`Bestellen')}

Mit der Vollversion erhalten Sie weiterhin SpyProtector, der Sie vor den häufigsten Überwachungenarten schützt. SpyProtector verhindert die Aufzeichnung von Tastatureingaben, Mausbewegungen, Programmstarts und warnt bei Autostart-Registryänderungen. Die Vollversion beinhaltet eine kostenlose Updatemöglichkeit auf alle 1.x Versionen. Alles gute Gründe, Security Task Manager noch heute zu kaufen.

Willkommen zur Vollversion

Wir begrüßen Sie recht herzlich als neuen, registrierten Security Task Manager Anwender.

Security Task Manager wird Ihnen bei der Analyse Ihres Computers gute Dienste leisten. Die Software SpyProtector, die Sie vor den häufigsten Überwachungenarten schützt, ist nun freigeschaltet. SpyProtector verhindert die Aufzeichnung von Tastatureingaben, Mausbewegungen, Programmstarts und warnt bei Autostart-Registryänderungen.

Bitte heben Sie Ihre Registrierdaten gut auf, da Sie hiermit auch zukünftige Versionen freischalten können.

Wenn Sie noch Fragen haben... 

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.

{button So funktioniert der Security Task Manager,JI(`taskman_de.hlp',`Konzept')}

{button ,AL("Info")} Siehe auch

So funktioniert Security Task Manager

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.

{button ,PI(`',`Name')} Name
{button ,PI(`',`Bewertung')} Bewertung
{button ,PI(`',`PID')} Prozess ID (PID)
{button ,PI(`',`CPU')} CPU
{button ,PI(`',`mem')} Speicher (RAM)
{button ,PI(`',`Aktiv')} Aktive Laufzeit
{button ,PI(`',`Datei')} Datei
{button ,PI(`',`Typ')} Typ
{button ,PI(`',`Start')} Start
{button ,PI(`',`Titel')} Titel und Beschreibung
{button ,PI(`',`Hersteller')} 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  **Systemprozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.

{button ,AL("Info;Anleitung")} Siehe auch

Ein Prozess bezeichnet ein Programm, Treiber, Dienst oder PlugIn - also jeden ausführbaren Code, der im Arbeitsspeicher Ihres Computers aktiv ist.

Zeigt den Namen der Software oder des Treibers an.

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.

Zeigt die Identifikationsnummer (ID) des Prozesses. Jeder Prozess besitzt eine eigene, eindeutige Nummer.

Zeigt den Pfad und den Namen der Datei.

Zeigt ob es sich um ein Programm, ein in der Taskleiste verankertes Programm, BHO, Treiber oder Dienst handelt.

von Security Task Manager unterschiedene Prozess Typen

Zeigt wann und durch wenn der Prozess gestartet wurde.

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.

Zeigt den Arbeitsspeicher-Bedarf eines Prozesses.

Zeigt die Zeit, in der das Programm seit dem Windows-Start aktiv gearbeitet hat. Zeiten, in der der Prozess inaktiv war, werden nicht mitgezählt.

Zeigt den Titel und die in der Datei enthaltene Datei-Beschreibung. Bei einem sichtbarem Fenster entspricht der Titel dem Text in der Titelleiste.

Zeigt den Namen des Herstellers und die in der Datei gespeicherte Produktbeschreibung.

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

{button ,PI(`',`Programm')} Programm

{button ,PI(`',`Taskicon')} Taskbar Icon

DLL Dateien

{button ,PI(`',`DLL')} DLL

{button ,PI(`',`ShellEx')} SheelExecute

Internet-PlugIns

 Browser Helpers Objects

Treiber und Dienste

 Gerätetreiber

 Dateitreiber

 Dienst (eigener Prozess)

 Dienst (eigener Prozess mit Desktop-Interaktion)

 Dienst (beteiligter Prozess)

 Dienst (betreiligter 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  **Systemprozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.

{button ,AL("Prozess")} Siehe auch

Der als Programm bezeichnete Prozess kann sichtbar (als normales Windows-Fenster) oder unsichtbar sein.

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.

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.

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.

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 führen Systemfunktionen auf unterer Hardware-Ebene zur Unterstützung anderer Programme aus.

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).

Treiber für das auf Windows NT basierende Dateisystem.

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

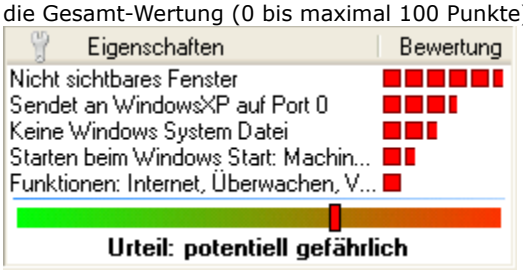
Ein System- oder Hardwarenaher Prozess zur Unterstützung anderer Programme. Der Dienst wird als eigener Prozess ausgeführt, der mit dem Desktop interagieren kann (z.B. Firewall, AntiVirus-Modul).

Der Dienst teilt sich mit anderen Diensten einen Prozess.

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):

{button ,PI(`',`B1')} Kann Tastatur Eingaben aufzeichnen
{button ,PI(`',`B2a')} Getarnter Prozess ist unsichtbar
{button ,PI(`',`B2')} Datei ist nicht sichtbar
{button ,PI(`',`B3')} Tastatur-Treiber, könnte Eingaben aufzeichnen
{button ,PI(`',`B4')} Kann andere Programme manipulieren
{button ,PI(`',`BHO')} Kann Internet Browser überwachen
{button ,PI(`',`ShellEx')} Startet beim Start anderer Programme
{button ,PI(`',`B5')} Lauscht auf Port *<Nr>*
{button ,PI(`',`B6')} Sendet an *<Computername>* auf Port *<Nr>*
{button ,PI(`',`B7')} Unbekanntes Programm lauscht oder sendet
{button ,PI(`',`B8')} Überwachen von Programmstarts
{button ,PI(`',`B9')} Nicht sichtbares Fenster
{button ,PI(`',`B10')} Starten beim Windows Start
{button ,PI(`',`B11')} Keine ausführlich Beschreibung vorhanden
{button ,PI(`',`B21')} Unbekannte Datei im Windows Ordner
{button ,PI(`',`B12')} Keine Windows System Datei
{button ,PI(`',`B13')} Fehlende Beschreibung des Programms
{button ,PI(`',`B14')} Funktionen: Internet, Überwachen, Eingabe aufzeichnen, Verstecken, Manipulieren
{button ,PI(`',`B15')} Funktionen: nicht ermittelbar
{button ,PI(`',`B16')} Unbekannter Hersteller

Vertrauenswürdige Eigenschaften (verbessern die Risiko-Bewertung):

{button ,PI(`',`B17')} Microsoft signierte Datei
{button ,PI(`',`B18')} Verisign signierte Datei
{button ,PI(`',`B20')} Gehört zu *<Software Produkt>* von *<Hersteller>*
{button ,PI(`',`B19')} Zertifiziert von *<Zertifizierungsstelle>* für Firma *<Hersteller>*
{button ,JI(`taskman_de.hlp>Proc1',`Kommentar')} 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 **Systemprozesse** in der Symbolleiste, um auch alle Windows-internen Prozesse zu sehen. Diese Prozesse gehören laut Microsoft zum Betriebssystem.

{button ,AL("Bewertung")} Siehe auch

Diese Eigenschaft scheint nicht sicherheitskritisch zu sein. Möchten Sie mehr über den Prozess erfahren, so nutzen Sie bitte die Internet-Suche.

Der Prozess überwacht jede Tastatureingabe. Per Hook werden die Eingaben mitgelesen. Sauber programmierte, seriöse Programme nutzen diese Hook-Funktion nicht.

So blocken Sie die Tastaturüberwachung

Der Prozess tarnt sich durch Windows API Hooking. Interne Windows Systembefehle zum Auflisten von Prozessen werden manipuliert. Er ist deshalb im Windows TaskManager oder mit anderen Prozess-Viewern nicht zu finden. Wir empfehlen, diesen Prozess unter Quarantäne zu stellen.

Die Datei versteckt sich vor dem Windows Explorer. Die Datei ist mit einem Dateimanager nicht zu sehen. Bitte nicht verwechseln mit dem harmlosen Dateiattribut "versteckt".

Es handelt sich um einen Tastatur-Treiber, der jede Eingabe mitlesen kann.

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.

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.

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.

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.

Der Prozess zeichnet auf, wann welche Programme aufgerufen und beendet werden.

Das Programm hat kein sichtbares Windows Fenster und läuft im Hintergrund. Im günstigsten Fall handelt es sich z.B. um Gerätetreiber.

Das Programm wird bei jedem Windows-Start aufgerufen. Hierzu hat sich das Programm in einen Autostart-Schlüssel inder Windows Systemregistrierung eingetragen.

Warnen beim Ändern der Registry

Einige wichtige Standard-Beschreibungen in der Datei wurden nicht gefunden. Standardmäßig enthält jede Datei intern Felder für Beschreibungen.

Die Datei gehört nicht zum Windows Betriebssystem. Sie wurde in das Windows-Verzeichnis kopiert, aber nicht korrekt angemeldet. Dies kann an einer schlecht programmierten Software liegen oder die Datei versucht sich im Windows-Verzeichnis zu verstecken.

Vorsicht ist geboten, wenn Sie diese Datei keinem installierten Software-Produkt oder Hardware-Treiber zuordnen können.

Die Datei gehört nicht zum Windows Betriebssystem. Erhöhte Aufmerksamkeit ist erforderlich, wenn sich die Datei im Windows Verzeichnis befindet und sich diese Datei keinem installierten Software-Produkt oder Hardware-Treiber zuordnen lässt.

Es wurden keine Beschreibungen in der Datei gefunden. Standardmäßig enthält jede Datei intern einige Felder für Beschreibungen.

Die Datei enthält Funktionsaufrufe mit den angegebenen Eigenschaften. Da jedoch nicht gesagt werden kann, ob und wie diese zum Einsatz kommen, wichtet der Security Task Manager dieses Kriterium nicht stark.

In der Datei wurden keine gefährlichen Funktionsaufrufe gefunden. Diese könnten jedoch versteckt integriert sein.

Der Hersteller ist nicht ermittelbar. Standardmäßig enthält jede Datei intern Felder zur Angabe des Softwareherstellers.

Diese Datei wurde von Microsoft signiert. Sie können dieser Datei vertrauen, so wie Sie auch Microsoft vertrauen.

Diese Datei wurde von VeriSign signiert. Sie können dieser Datei vertrauen, so wie Sie auch VeriSign vertrauen.

Diese Datei wurde von einer Zertifizierungsstelle signiert. Sie können dieser Datei vertrauen, so wie Sie auch der Zertifizierungsstelle und dem Softwarehersteller vertrauen.

Diese Datei ist als vertrauenswürdig eingestuft. Sie gehört zu der genannten, installierten Software. Wenn Sie die Software in der Systemsteuerung deinstallieren, so löschen Sie auch diese Datei.

So sehen Sie Details eines Prozesses

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

{button ,PI(`',`Name')} Name
{button ,PI(`',`Bewertung')} Bewertung
{button ,PI(`',`Hersteller')} Hersteller
{button ,PI(`',`Titel')} Beschreibung
{button ,PI(`',`Typ')} Typ
{button ,PI(`',`Start')} Start
{button ,PI(`',`Datei')} Datei
{button ,JI(`taskman_de.hlp>Proc1',`Kommentar')} Kommentar

So erhalten Sie noch mehr Informationen oder stoppen den Prozess:

 Informationen aus dem Web zu diesem Prozess

 Prozess beenden

 Prozess unter Quarantäne stellen

 **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 zusätzlichen Eigenschaften als Spalten in der Prozess-Liste angezeigt werden.

{button ,AL("Prozess")} Siehe auch

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:

{button ,PI(`',`Name')} Prozess beenden

{button ,PI(`',`Bewertung')} Datei in Quarantäne-Ordner verschieben

Anmerkung

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

{button ,AL("Prozess")} Siehe auch

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.

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.

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**.

{button ,AL("Beenden")} Siehe auch

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.

{button ,AL("Prozess")} Siehe auch

So exportieren Sie die Prozess Liste

1 Klicken Sie im Menü Datei auf **Exportieren nach**.

2 Wählen Sie als Dateityp:

{button ,} Website (*.html)

{button ,} Text file (*.txt)

Anmerkung

- Windows-Systemprozesse werden standardmäßig nicht angezeigt und demzufolge nicht exportiert. Klicken Sie auf den Button **Systemprozesse** 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 ausfindig zu machen. Eine gespeicherte Prozess Liste kann auch als Beweissicherung dienen.

{button ,AL("Speichern")} Siehe auch

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

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

{button ,AL("Speichern")} Siehe auch

So 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.

{button ,AL("Shareware")} Siehe auch

Schützen Sie sich mit SpyProtector

Kaufen Sie noch heute Security Task Manager und erhalten Sie gratis die Software SpyProtector mit dazu. SpyProtector bieten Ihnen folgende Werkzeuge, um sich vor Keyloggern, Spyware und Trojanern zu schützen:

- Datei- und Internetspuren löschen
- Überwachung von Tastatureingaben verhindern
- Überwachung von Mausklicks verhindern
- Überwachung von Programmstarts verhindern
- Warnen bei Autostart-Registryänderung

{button Security Task Manager jetzt kaufen,JI(`taskman_de.hlp',`Bestellen')}

{button ,AL("Shareware")} Siehe auch

Die Software SpyProtector kann für die aktuelle Windows Sitzung Überwachungsprogramme unschädlich machen werden, die heimlich alle Mausbewegungen und Mausklicks aufzeichnen. Die Überwachung der Maus durch Fremprogramme wird wie bei einer Firewall blockiert.

SpyProtector kann für die aktuelle Windows Sitzung Überwachungsprogramme unschädlich machen, die das Aufrufen und Schließen von Programmen protokollieren.

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

- ✔ Tastaturaufzeichnung nicht erlauben
- ✔ Andere Überwachungen nicht erlauben
- ✔ Warnen bei Autostart-Registryänderung

{button ,AL("Schutz")} Siehe auch

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.

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.

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.

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.

- To read how to change the language please click here .

{button ,AL("Sprache")} Siehe auch

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.

{button ,AL("Sprache")} Siehe auch

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

---

{button ,AL("Info;Shareware")} Siehe auch

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, 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.

{button ,AL("Team;Shareware")} Siehe auch

So bestellen Sie Ihren Freischaltcode

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.

{button ,AL("Shareware;Team")} Siehe auch

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

- Bei Fragen, wenden Sie sich bitte an uns.
- Ihren Freischaltcode erhalten Sie innerhalb von 24 h.

{button ,AL("Shareware")} Siehe auch

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

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

Falscher Name oder falscher Freischaltcode!
Geben Sie hier Ihre Adresse genau so ein, wie diese in Ihren Registrierunterlagen geschrieben steht.
Beachten Sie die Groß- und Kleinschreibung.