20.11.2011 - Diese Programme laufen heimlich auf jedem PC

ChannelPartner : Ratgeber

Speicherfresser und Spione - auf jedem PC laufen versteckte Programme. Mit den Tipps unserer Schwesterzeitschrift PC Welt befreien Sie PCs Ihrer Kunden von getarnten Schädlingen und Ballast.

Versteckte Prozesse finden: Wer glaubt, die Taskbar zeigt alle aktuell laufenden Programme an, der irrt sich gewaltig. Im Hintergrund laufen wesentlich mehr Anwendungen, als Windows per Taskbar-Icon preisgeben will. Einen ersten Überblick verschaffen Sie sich mit dem Task-Manager.

Unter "Anwendungen" zeigt der TaskManager die momentan geöffnete Software an - hier dürften Sie keine Überraschungen erleben. Per "Task beenden" schließen Sie das ausgewählte Programm (Vorsicht, Datenverlust!). Spannender ist der Reiter "Prozesse": Hier listet Windows alle laufenden Prozesse sortierbar nach Name, Nutzer, CPU-Auslastung und Speicherauslastung.

Finden und Beseitigen Sie Speicherfresser und Spione auf Ihrem PC.

Tipp: Die Freeware Process Explorer zeigt auch Prozesse, die der Windows-Task-Manager verschweigt. Viele Prozesse haben ungewohnte Namen - oft gibt erst eine Google-Suche Auskunft über Funktion und Nutzen. Längst nicht alle Prozesse sind zwingend notwendig - einige bremsen den PC sogar nur unnötig aus.

Bequem und sicher unnötige Hintergrund-Prozesse abschalten

Die Dienste einfach zu beenden ist gefährlich - insbesondere, wenn es sich um einen Microsoft-Dienst handelt, den Windows womöglich dringend benötigt. Mit einem Trick blenden Sie alle Microsoft-Dienste aus. Drücken Sie gleichzeitig die Windows-Taste und "R". Geben Sie "msconfig" in das Ausführen-Feld ein und bestätigen Sie mit Enter. Im Reiter "Dienste" sehen Sie nicht nur bereits beendete Dienste und Hersteller-Namen, sondern auch eine Klickbox, die alle Microsoft-Dienste ausblendet. Damit haben Sie zwar eine potentielle Gefahr gebannt, es ist jedoch mindestens genauso schlimm, wenn Sie etwa die Antiviren-Software unabsichtlich beenden.

Die exklusiven PC-WELT-Tools pcw-XPServices für Windows XP beziehungsweise pcwVistaServices für Vista erleichtern das Deaktivieren unbenötigter Programme, die heimlich im Hintergrund laufen. Bevor Sie sich für die PC-WELT-Empfehlung oder die absolute Minimal-Konfiguration der Hintergrund-Dienste entscheiden, sollten Sie die aktuelle Konfiguration mit Hilfe des entsprechenden Buttons sichern. Läuft etwas schief - wenn etwa ein Programm den Dienst verweigert - stellen Sie die funktionierende Konfiguration oder die Standard-Einstellung per Mausklick wieder her.

Rootkits - Schutz vor der unsichtbaren Gefahr

Rootkits sind Schädlinge, die sich vor dem Windows-Nutzer und selbst der Antiviren-Software tief im System verstecken. Rootkits manipulieren den Kern des Betriebssystems oder laufende Prozesse so, dass sie weder für den Windows-Explorer noch einen anderen Dateimanager sichtbar sind. Ein Blick in den Task-Manager wäre also vergebliche Liebesmüh.

Besonders raffiniert programmierte Rootkits verstecken sich sogar im Master Boot Record. Dieses MSDOS-Zeiten-Überbleibsel wird beim Start des Rechners geladen, noch vor dem Betriebssystem. Dort sitzender Code kann im Prinzip das Betriebssystem kontrollieren. Erst ab Windows Vista erlauben Microsoft-Betriebssysteme die Manipulation des Master Boot Record nicht mehr im laufenden Betrieb - zumindest nicht ohne Weiteres. Ziel der meisten Rootkits: Spyware und Trojaner tarnen, die dann persönliche Daten ins Netz schicken.

Ein guter Schutz vor Rootkits ist das Arbeiten und Surfen unter einem Benutzerkonto mit eingeschränkten Rechten. Viele Rootkits können sich nur mit Admin-Rechten ins System einklinken, erstellen Sie also ein neues Benutzerkonto mit eingeschränkten Rechten, falls noch nicht geschehen. Außerdem sollten Sie eine Zwei-Wege-Firewall verwenden. Denn diese meldet nicht nur eingehende Verbindungen, sondern auch Programme, die nach draußen funken wollen. Es gibt aber auch Tools, die bereits eingeschlichene Rootkits finden und eliminieren.

Gut: In einem aktuellen Test von elf Antiviren-Programmen zeigte sich keines ohne Rootkit-Schutz. Besonders zuverlässig fanden und entfernten etwa Norton Antivirus 2011,

Kaspersky Antivirus 2011 und McAfee Antivirus Plus 2011 unsere zehn Test-Rootkits. Aber auch G-Data Antivirus 2011, Bitdefender 2011, F-Secure Antivirus 2011, Panda Antivirus Pro 2011 und Avira Antivir Premium überzeugten in dieser einzelnen Disziplin mit guten Ergebnissen. Eine Auflistung von gängigen Firewall-Lösungen, die mitunter auch ein Virenschutz-Programm mitbringen, können Sie der untenstehenden Galerie entnehmen

Quelle / Links zum Thema:

- Vollständiger Ratgeber auf ChannelPartner.de

09.12.2010 - Backups von Festplatten

Neben der E-Mailarchivierung und dem Backup der E-Mailordner werden in einem Unternehmen in aller Regel auch Backups der Festplatten der lokalen Rechner der einzelnen Mitarbeiter erstellt.

Auf der lokalen Festplatte können private Dateien des Arbeitnehmers (Fotos, Textdokumente etc.) gespeichert sein. Die Dateien kann der Arbeitnehmer auf dem Rechner originär erstellt, von einem externen Datenträger auf ihn übertragen oder durch Herunterladen aus dem Internet oder aus einer E-Mail auf ihm gespeichert haben.

Sollte die Datei aus einer privaten E-Mail heruntergeladen worden sein, zählt sie zwar zum Inhalt einer Fernkommunikation, jedoch unterliegt sie nicht mehr dem Fernmeldegeheimnis, da dieses endet, wenn die Übermittlung der Kommunikation beendet ist. Dies ist hier der Fall. Die Datei ist nun im alleinigen Herrschaftsbereich des Arbeitnehmers. Dies gilt unabhängig davon, ob die E-Mail samt Datei noch auf einem Server des Arbeitgebers liegt. Denn die E-Mail und Datei auf dem Server des Arbeitgebers ist immer noch vom Fernmeldegeheimnis geschützt.

Für die privaten Dateien, die der Arbeitnehmer auf seinem Rechner gespeichert hat, gilt dann das Bundesdatenschutzgesetz. Dann können wiederum individuelle Einwilligungen eingeholt oder eine Betriebsvereinbarung über das Backup geschlossen werden.

Schließlich kann das Backup auch durch § 32 BDSG gerechtfertigt werden, wenn das Backup ein für die Durchführung des Arbeitsverhältnisses erforderliche Maßnahme ist. Erforderlich ist die Verwendung personenbezogener Daten dann, wenn keine objektiv zumutbare Alternative existiert. Die Erforderlichkeit ist anzunehmen, wenn die berechtigten Interessen des Arbeitgebers auf andere Weise nicht oder nicht angemessen gewahrt werden können. Es ist eine Interessensabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes (Art. 14 I GG) vorzunehmen.

Der Arbeitgeber hat ein berechtigtes Interesse daran, die Festplatten zu backupen, da dort wichtige Dokumente der Arbeit (wie Verträge, Vereinbarungen, Präsentationen, Fotos, Memos usw.) liegen, die nicht verloren gehen dürfen oder sollen. Die Abwägung fällt dahingehend aus, dass der Datenschutz zurücktreten muss. Ihm kann aber ausreichend Raum geschaffen werden, indem auf der Festplatte eines jeden lokalen Rechners ein Ordner "Privat" eingerichtet wird, der nicht gebackupt wird. Speichert ein Arbeitnehmer eine Datei dann nicht im Ordner "Privat", verstößt er gegen seine Arbeitnehmertreuepflicht und ist nicht mehr schutzwürdig. (oe)

LESEN SIE AUCH »

- Arbeitnehmerdaten: Die datenschutzrechtliche Einwilligung im Arbeitsverhältnis
- Datenschutz am Arbeitsplatz: Nutzung von PC, Telefon und E-Mail der Firma
- Ratgeber für Reseller: So archivieren Sie E-Mails revisionssicher

Patrick Prestel und Max-Lion Keller, LL.M. (IT-Recht) arbeiten bei der IT-Recht Kanzlei, Alter Messeplatz 2, 80339 München, Tel.: 089 1301433-0 , E-Mail: m.keller@it-recht-kanzlei.de, Internet: www.IT-Recht-Kanzlei.de

Quelle : ChannelPartner