Was macht eigentlich ein AntiVirus-Programm?

Wenn Sie ein aktuelles AntiVirus-Programm installieren und die während der Installation vorgeschlagenen Einstellungen vom Informationsassistenten übernehmen, ist Ihr Computer mit den üblichen und grundlegenden Standart-Funktionen vor Viren geschützt. Zusätzliche Einstellungen, die man in den unterschiedlichen

Vor der Installation sollte der betreffende PC auf mögliche Viren hin geprüft werden. Alternativ hilft da auch ein Online-Virencheck, der bei führenden Herstellern von AntiViren-Software verfügbar ist. (z. B. unter www.Symantec.com)

Während der Installation wird der Computer auf Viren geprüft. Dabei werden aber nur die Viren erkannt, die zum Zeitpunkt der Herstellung vom Antiviren-Programm durch die Virensignaturen bekannt waren.

AntiVirus-Programme führen folgende Aufgaben automatisch aus:

- ⇨ Prüfung von Boot-Sektoren beim Systemstart auf Viren (*ältere Programme haben Probleme, unter Windows NT, Windows 2000, Windows XP und Windows Me diese Prüfung auszuführen*).
- ⇨ Prüfung der Programme beim Starten auf Viren,
- ⇨ einmal wöchentlich automatische Überprüfung aller lokalen Laufwerke auf Viren,
- ⇨ Überwacht den Computer auf Aktivitäten, die auf einen aktiven Virus hinweisen könnten,
- ⇨ Überprüfung externer Datenträger auf Boot-Sektor-Viren beim Datenzugriff,
- ⇨ Prüfung eingehender und ausgehender E-Mails auf Viren und verhindert dadurch, dass E-Mails, die Viren enthalten, empfangen oder gesendet werden

Mit AntiVirus-Programmen können Dateien, Ordner oder Laufwerke auf Viren geprüft werden. Aufgefundene infizierte Dateien können dann isoliert werden, um sie per Onlineverbindung an die jeweiligen Hersteller der Antiviren-Software zu senden. Gesendete Dateien werden dort von den Experten analysiert. Die Ergebnisse werden dann automatisch innerhalb weniger Tagen zurückgesandt.

Auto-Protect = Überwacht Aktivitäten, die auf einen aktiven Virus hinweisen könnten

- entdeckt alle Virustypen, darunter Makroviren, Boot-Viren, speicherresidente Viren und Trojanische Pferde, Würmer und anderer bösartiger Code, und schützt das PC-System vor diesen
- schützt den Computer vor über das Internet übertragenen Viren, indem es alle von Ihnen aus dem Internet heruntergeladenen Dateien, z. B. Java Applets oder ActiveX-Controls, überprüft
- prüft jedesmal auf Viren, wenn ein Softwareprogramm auf dem Computer gestartet wird,
- prüft eingelegte Disketten oder andere Wechselmedien bei Zugriff
- prüft Dokumente, die geändert oder geöffnet werden,

- überprüft den Computer auf ungewöhnliche Aktivitäten, die auf einen aktiven Virus hinweisen könnten

Durch den aktivierten Auto-Protect wird ein dauerhafter Virenschutz gewährleistet. Auto-Protect startet selbstständig, wenn das Windows-Betriebssystem auf dem Computer gestartet wird.

Infizierte Dateien sollten zuerst repariert werden. Erst dann, wenn diese Option nicht erfolgreich verlief, sollten diese Dateien isoliert werden. Dadurch wird der weitere Zugriff auf die infizierte Datei verweigert und somit verhindert, dass Sie oder andere Programme auf Ihrem Computer die infizierte Datei öffnen. Die isolierten Dateien werden nicht repariert, können jedoch keine anderen Dateien auf Ihrem Computer infizieren.

E-Mail-Prüfung

Das Senden von E-Mails ist heute ein wesentlicher Bestandteil der täglichen Kommunikation. Die Verbreitung von Viren, die dann Ihren Computer infizieren, findet in den meisten Fällen via E-Mail statt. Aktuelle AntiVirus-Programme unterstützen alle E-Mail-Programme, die POP3 und SMTP-Protokolle verwenden. Nach der Installation konfiguriert das AntiVirus-Programm Ihr E-Mail-Programm automatisch so, dass es vor Viren geschützt ist.

Skriptblockierung

Die Skriptblockierung überwacht skriptbasierte Viren und warnt bei virusähnlichen, bösartigen Aktivitäten, wobei die Skriptblockierung die Viren aufhält, bevor diese Ihr System infizieren können.

Skripts werden häufig verwendet, um legale Programme zu schreiben, sie können aber auch so verfasst werden, dass sie schädliche Aktivitäten ausführen. Virenprogrammierer verwenden zunehmend Technologien zur Skripterstellung wie JavaScript oder VBScript, um Ihr Computersystem infizieren zu können. Sie können, ohne es zu merken, ein schädliches Skript erhalten, indem Sie ein infiziertes Dokument oder einen infizierten E-Mail-Anhang öffnen, eine infizierte HTML-E-Mail-Nachricht anzeigen oder eine infizierte Internet-Website besuchen.

Die Skriptblockierung bietet Ihnen nun Schutz vor sich schnell ausbreitenden Viren wie "I Love You" oder "Anna Kournikova", selbst dann, wenn noch keine Virendefinitionen verfügbar sind. Dies ist besonders in der heutigen Zeit, in der immer mehr Computer in Netzwerken miteinander verbunden sind, von großer Bedeutung, da solche Viren sich wesentlich schneller ausbreiten können als die entsprechenden Schutzmaßnahmen, die in der Regel in Form von Signaturen oder Virendefinitionen vorliegen. Die Skriptblockierung ist eine proaktive Technologie, die skriptbasierte Viren auch ohne Signaturen erkennt.

Vollständige Systemprüfung

Anhand des Status der vollständigen Systemprüfung können Sie sehen, ob Sie eine Virusprüfung auf Ihrem Computer durchgeführt haben. Bei einer vollständigen Systemprüfung werden alle Boot-Sektoren, Master-Boot-Sektoren und alle Dateien auf Ihrem Computer geprüft. Es ist wichtig, nach der er-

sten Installation eine vollständige Systemprüfung durchzuführen, um sicherzustellen, dass sich keine Viren in Ihrem System befinden.

Während der Installation, können Sie festlegen, dass jede Woche eine vollständige Systemprüfung durchgeführt werden soll. Wenn Sie diese Option aktivieren, wird die Prüfung automatisch geplant. Sie können die Angaben für die geplanten Prüfungen jederzeit überarbeiten und ändern oder die Prüfungen neu planen.

Virendefinitionen

Im Status der Virendefinitionen wird angezeigt, ob Ihre Virendefinitionen aktuell sind und wann die Virendefinitionen, die sich auf Ihrem Computer befinden, erstellt wurden. Virendefinitionen enthalten bestimmte Signaturinformationen, anhand derer das jeweiligen AntiViren-Programm Viren und bösartigen Code entdecken und Sie davor schützen kann.

Die Anti-Viren-Experten der bekannten Hersteller forschen ständig nach Viren und bösartigem Code und sorgen so dafür, dass regelmäßig neue Virendefinitionen herausgegeben werden können und Ihr System jederzeit bestmöglich geschützt ist. Damit Ihr Computer nicht durch neue Viren infiziert wird, sollten Sie Ihr Anti-Virus Abonnement ständig erneuern und regelmäßig Ihre Virendefinitionen aktualisieren.

Automatisches LiveUpdate

Anhand des Status für das automatische LiveUpdate können Sie sehen, ob die LiveUpdate-Funktion aktiviert ist. Sie sollte stets aktiviert sein, um sicherzustellen, dass das AntiVirus-Programm immer mit den neuesten Virendefinitionen arbeitet. Virendefinitionsdateien enthalten Virusinformationen, anhand derer das Programm Viren entdeckt und Sie entsprechend warnen kann.

Durch das automatische LiveUpdate werden regelmäßig neue Virendefinitionen per Online-Verbindung dem AntiVirus-Programm auf den Computer zur Verfügung gestellt. Nach dem automatischen Download der neuen Virendefinitionen startet im Anschluss selbstständig die Installation zum AntiVirus-Programm. Dadurch wird sichergestellt, dass das AntiVirus-Programm immer auf dem neusten Stand der Signaturen bleibt und dadurch neue Viren erkennen, reparieren bzw. isolieren kann.

Bloodhound-Optionen / Heuristik

AntiVirus-Programme verfügen über eine Technologie, die sogenannte "Bloodhound-Technologie", durch die der Virenschutz bei schwierig zu erkennenden Viren entscheidend verbessert wird.

Durch diese Technologie werden die unterschiedlichen logischen Bereiche einer Datei isoliert und ermittelt. Anschließend wird die Programmlogik auf virusähnliches Verhalten hin untersucht. Die Bloodhound-Technologie ist in der Lage, die meisten unbekannten Viren zu entdecken. Außerdem kann das Programm unbekannte Viren entdecken, indem es die Aktivitäten auf Ihrem Computer auf Verhaltensweisen überwacht, die für Viren typisch sind. Wenn verdächtige Aktivitäten entdeckt werden, hält das AntiVirus-Programm die Aktion an.