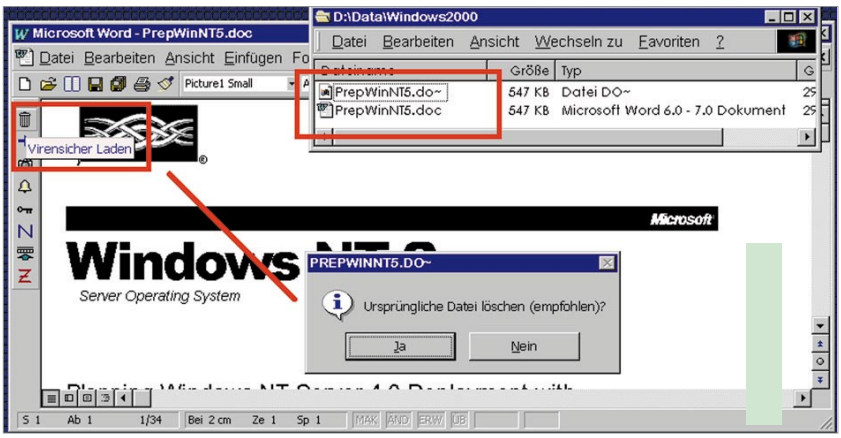
Ein Makro schützt vor Virenmakros

Word: Virenfrei!

Word-Makroviren sind derzeit die PC-Seuche Nummer 1. Lesen Sie, wie Sie ihnen komfortabel und absolut sicher aus dem Weg gehen



Antiviren-Makro (Papierkorb-Icon): Sie laden Word-Dateien damit garantiert makrovirenfrei und behalten auf Wunsch Kopien der Ursprungsversionen

Als die ersten Word-Viren vor vier Jahren auftauchten, belächelten Experten sie zunächst als exotische Konstrukte. Inzwischen führen sie Monat für Monat die Top-Listen der meistverbreiteten Viren an. Hinzu kommen noch die vermutlich zahllosen Makro-Trojaner, die in Firmennetzen ihr Unwesen treiben und von keiner Statistik erfaßt werden.

Wir zeigen auf, welche Nachteile die Methoden haben, die üblicherweise zum Schutz vor Viren benutzt werden – und stellen Ihnen dann eine absolut zuverlässige Methode vor, mit der Sie Word-Viren stoppen und verseuchte Dokumente säubern.

UNBEQUEM ODER UNSICHER

Makrovirus-Schutz, Antiviren-Software & Co.

Ab Word 97 ist standardmäßig der **„Makrovirus-Schutz"** aktiviert (siehe „Extras, Optionen, Allgemein"). Er erkennt, ob eine Word-Datei Makros enthält, und bietet die Option, diese Makros zu deaktivieren. Dieser Mechanismus hat zwei Nachteile:

1. Der Makrovirus-Schutz meldet sich nur, wenn sich in der Datei selbst Makros verbergen. Ist eine Datei jedoch mit einer Dokumentvorlage verknüpft, die Makros enthält, versagt er komplett. Das läßt sich auch nicht ändern, da der Anwender sonst ständig den Schutzdialog vor Augen hätte, sobald seine Standardvorlage NORMAL.DOT auch nur ein einziges Makro besitzt. Diese Sicherheitslücke ist um so brisanter, als eine verknüpfte Dokumentvorlage keineswegs die Erweiterung DOT besitzen muß: Wenn Sie etwa ein E-Mail-Attachment mit den Dateien HALLO.DOC und HALLO.BMP erhalten, kann die angebliche Bilddatei (BMP) eine verkappte Dokumentvorlage sein. Beim Öffnen der DOC startet Word dann die Makros der BMP-Datei – der Dateiname spielt dabei keine Rolle.

2. Wer selbst programmiert, muß mit ständigen Warnungen vor eigenen Makros leben. Dies wird fleißigen Makro-Benutzern schnell lästig.

Auch der Einsatz von **Antiviren-Programmen** hat Nachteile:

1. Trotz heuristischer Scan-Methoden finden die Programme meist nur bekannte Schädlinge. Bei geändertem Virencode und neuen Trojaner-Makros sind sie in der Regel hilflos.

2. Makroviren aus befallenen Dateien zu entfernen gelingt nicht allen Programmen. Noch am besten schnitt in einem Testlauf Norton Antivirus 5.0 ab.

3. Es erfordert Disziplin, alle neuen Dateien konsequent zu scannen und die Signaturen aktuell zu halten.

Der bekannte Tip, das Ausführen von selbststartenden Makros (Autoopen, Autoclose) über ein eigenes Autoexec-Makro zu verbieten, schützt nur vor einer bestimmten Sorte Viren (eben nur den selbststartenden). Gegen ein Virus-Makro, das einen Standardbefehl wie „Datei, Öffnen" umdefiniert, bietet diese Methode keinen Schutz.

SIMPEL UND SICHER

„Einfügen, Datei" statt „Datei, Öffnen"

Bereits vor einem Jahr (siehe „Tips: Windows 95/98", PC-WELT 9/98, Seite 90, Tip 2; Tip auch **auf Heft-CD**) verwiesen wir auf eine sichere Möglichkeit, Word-Viren mit Word-Mitteln zu entschärfen: Laden Sie in Word eine Datei über „Einfügen, Datei", dann erhalten Sie den Text mit Formatierungen, Bildern, Gliederungselementen – aber garantiert ohne Makros, also auch ohne eventuell enthaltene Viren. Lediglich die Seiteneinstellungen basieren dann auf der NORMAL.DOT und müssen eventuell angepaßt werden.

Um diese Methode komfortabel zu machen, haben wir ein Makro produziert, das automatisch dafür sorgt, daß die eingefügte Datei unter dem ursprünglichen Namen gespeichert wird. Ferner empfehlen wir ein DDE-Makro in der Registry, um auch im Windows-Explorer das virenfreie Laden zu gewährleisten.

DAS WORD-MAKRO (I)

So integrieren Sie den Schutz

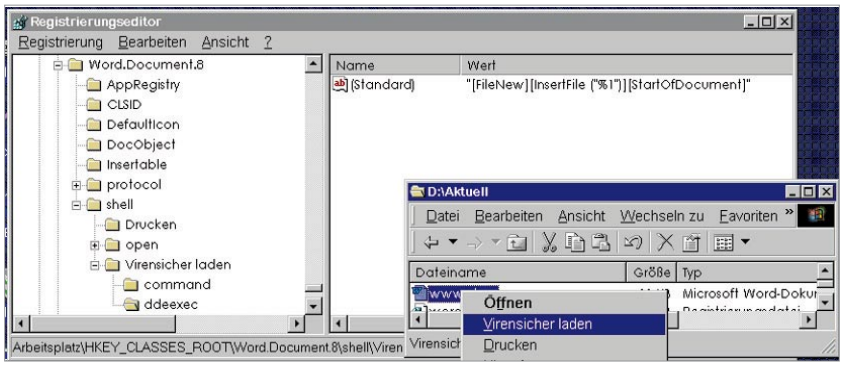
Die Datei Virensicher.DOT (unter *www.pcwelt.de* und auch **auf Heft-CD**) enthält das Makro „Virensicher Laden“. Starten Sie Word (6, 95, 97, 2000), und öffnen Sie Virensicher.DOT mit „Datei, Öffnen“. Falls der Virenschutz-Dialog erscheint, klicken Sie auf „Makros aktivieren“. Danach wählen Sie „Extras, Makro, (Makros,) Organisieren“. In diesem Dialog klicken Sie auf die Schaltfläche „Kopieren“, um „Virensicher Laden“ in die Standardvorlage NORMAL.DOT zu übertragen. Danach beenden Sie den Dialog mit dem Button „Schließen“. Das Makro ist nun global verfügbar, aber noch nicht in die Oberfläche integriert. Passende Orte sind die Symbolleiste oder das Menü „Datei“. Der Einbau des Makros unterscheidet sich in den verschiedenen Word-Versionen geringfügig:

Word 6 und 95: Wählen Sie „Extras, Anpassen“, dann je nach Geschmack das Register „Symbolleisten“ oder „Menüs“. Unter „Kategorien“ klicken Sie auf den Eintrag „Makros“, dann auf „VirensicherLaden“. Das Integrieren in eine Symbolleiste geht jetzt per Drag & Drop. In der folgenden Dialogbox bestimmen Sie eine Schaltfläche Ihrer Wahl.

Um den Befehl in das Menü „Datei“ aufzunehmen, wählen Sie im Feld „Menü ändern“ den Eintrag „&Datei“. Dann können Sie manuell Position und Namen des neuen Menüeintrags definieren.

Word 97 und 2000: Unter „Extras, Anpassen“ markieren Sie die Kategorie „Makros“. Das Makro „VirensicherLaden“ ziehen Sie auf eine Symbolleiste oder direkt auf das Menü „Datei“. Lassen Sie im zweiten Fall die Maus erst los, wenn das Menü „Datei“ aufgeklappt und die gewünschte Position erreicht ist. Nach Rechtsklick auf das neue Symbol oder den neuen Menüeintrag ändern Sie Namen und Aussehen nach Ihrem Geschmack.

Sie können jetzt den Dialog „Anpassen“ schließen. Um die Änderungen dauerhaft zu speichern, wählen Sie „Datei, Alles speichern“.



Neuer Kontextmenü-Eintrag: Das DDE-Makro komplettiert den Virenschutz, indem es Word-Dateien über den Windows-Explorer virenfrei lädt

DAS WORD-MAKRO (II)

Wie das Makro funktioniert

Verwenden Sie den neuen Befehl immer, wenn Sie Word-Dateien aus fremden Quellen (Netz, E-Mail, Internet, Diskette) lesen oder weiterbearbeiten wollen. Sie schützen sich damit aber nicht nur vor Makroviren. Sie können virenverseuchte Dateien auch bequem säubern, denn die Virus-Makros werden zuverlässig gelöscht: Das Makro öffnet zunächst den Dialog „Datei, Einfügen“, um Sie die fragliche Datei per Doppelklick auswählen zu lassen. Danach benennt es die Datei um, indem es die Extension DO~ vergibt, fügt den Text virenfrei in ein neues Fenster ein und speichert ihn unter dem Originalnamen. Ob Sie die ursprüngliche Datei (*.DO~) behalten oder löschen wollen, entscheiden Sie im nachfolgenden Dialog.

DAS DDE-MAKRO

Virensicher auch im Explorer

Den Schutz perfekt macht ein Eingriff in die Registry: DOC-Dateien erhalten im Explorer ein zusätzliches Kontextmenü, über das Sie Word-Dateien ebenfalls virensicher öffnen.

Theoretisch sollte es möglich sein, das Word-Makro als DDEEXEC-Makro in der Registry anzulegen. Allerdings stürzen die Versionen 97 und 2000 (mit VBA – Visual Basic for Applications) ab, wenn ein DDEEXEC-Makro (englisches Wordbasic) länger ist als 255 Zeichen. Da der Dateiname als Parameter übergeben wird, variiert die Länge des Makros. Daher ist es unmöglich, ein komplexes und absturzsicheres DDEEXEC-Makro anzulegen. Wir mußten uns hier deshalb auf das absolut Notwendige beschränken:

```
[DateiNeu][EinfügenDatei
  ("%1")][BeginnDokument]
```

Diese Zeile gilt für das deutschsprachige Word 6 und 95; für Word 97 und 2000 sowie das englischsprachige Word 6 und 95 hingegen:

```
[FileNew][InsertFile
  ("%1")][StartOfDocument]
```

Starten Sie REGEDIT.EXE, und suchen Sie unter „Hkey_Classes_Root“ die Extension „.DOC“. Rechts sehen Sie den Schlüssel für die aktive Word-Version (etwa „Word.Document.8“). Gehen Sie zu diesem Schlüssel. Markieren Sie dort „Shell“, und erstellen Sie den neuen Schlüssel „Virensicher laden“, darunter die beiden Schlüssel „command“ und „ddeexec“ (diese beiden hierarchisch gleichgeordnet). Für „command“ definieren Sie als „Standard“ Pfad und Namen zur WINWORD.EXE und setzen dahinter den Parameter /n (lädt Word ohne ein Dokumentfenster). Die Zeile übernehmen Sie am besten von \print\command unmittelbar darüber. Für „ddeexec“ fügen Sie als „Standard“ eine der beiden obengenannten Zeilen ein.

Achtung! Wenn Mail-Clients DOCs direkt an Word schicken, werden die beiden Schutzmaßnahmen natürlich umgangen. Sie sollten daher Attachments stets zunächst speichern und erst dann in Word virensicher laden.

HERMANN APFELBÖCK