

## Viren und Microsoft Office: Was taugen die Bordmittel?

Von Thomas Rieske / 17.06.2003

PCs mit Microsoft Office sind ein beliebtes Ziel von Virenangriffen. Das liegt zum einen daran, dass die Büro-Suite weltweit verbreitet ist und so jede Menge potenzieller Opfer vorhanden sind. Zum anderen ist Office insofern anfällig, als es mit Visual Basic für Applikationen (VBA) über eine mächtige Makrosprache verfügt.

Mit diesem Programmierwerkzeug lassen sich nicht nur Abläufe in Word & Co. automatisieren, sondern auch Systemaufrufe durchführen. Ein Makro kann daher Dateien manipulieren, weitere Programme starten oder sogar die Festplatte formatieren.

Angreifen sind damit Tür und Tor geöffnet. Nehmen wir einmal an, Sie haben eine umfangreiche Excel-Tabelle mit einer statistischen Auswertung erstellt. Ein Virus könnte hier nach dem Zufallsprinzip einige Vorzeichen vertauschen. Die Arbeit vieler Stunden oder gar Tage geht so verloren. Ein Virus könnte aber genauso gut in einem Word-Text einzelne Wörter ersetzen. Meist lassen sich die Originaldaten nur über ein aktuelles Backup wiederherstellen.

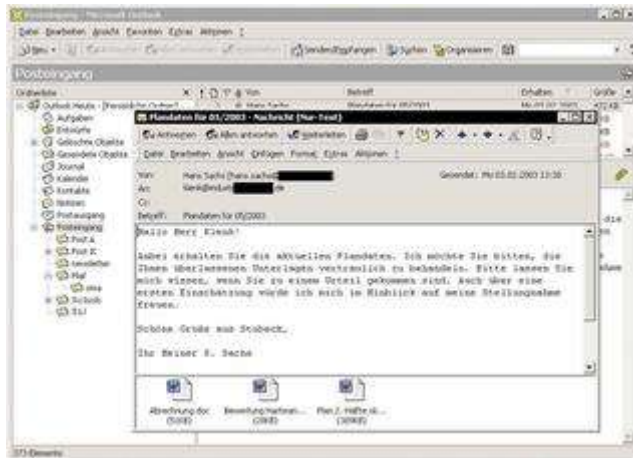
### Hauptgefahr Makroviren: Tarnen, täuschen, zuschlagen

Makroviren verbergen sich in Add-ins, Vorlagen und Dokumenten. Damit sie ihr zerstörerisches Werk beginnen können, sind sie immer darauf angewiesen, dass die entsprechende Anwendung gestartet und das infizierte Makro ausgeführt wird. Das passiert schneller, als man vielleicht denkt. Häufig erhalten Anwender Office-Dokumente als Anlage zu Mails oder stoßen beim Surfen im Internet darauf. Ein unbedachter Doppelklick genügt - und die Office-Anwendung startet.

Formularbeginn

/graphics/bild_db	Wo viele Anwen
-------------------	----------------

Formularende



[Wo viele Anwender per Attachment Dateien tauschen, ist die Gefahr, sich einen Virus einzufangen, besonders hoch. Ein genauer Einblick in den Datei-Anhang ist nicht möglich.](#)

Die meisten Makroviren verwenden so genannte Auto-Makros, die beim Öffnen einer Datei automatisch ablaufen. Andere benutzen oft ausgeführte Standardbefehle wie "Datei speichern" und ersetzen diese Aufrufe durch ihren Virencode.

Anschließend verbreiten sie sich ungehindert weiter, indem sie andere Dokumente und vor allem die Standardvorlage NORMAL.DOT in Word infizieren. Übrigens können Makroviren als Schleuser, so genannte Dropper, fungieren, die Ihren Rechner mit weiteren Viren, Würmern und Trojanern verseuchen.

**Vorbeugung: Misstrauen ist besser als Neugier**

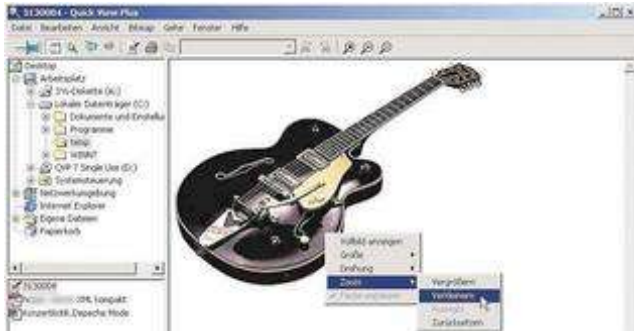
Es gibt durchaus einige Verhaltensregeln und Konfigurationsmaßnahmen, mit denen Sie die Gefahr einer Vireninfektion verringern können. An erster Stelle steht dabei ein gesundes Misstrauen insbesondere gegenüber Dateien, die Ihnen jemand unverlangt zuschickt oder die sich hinter interessant klingenden Link- Namen im Internet verbergen.

Anstatt Dokumente unbekannter Herkunft in Office zu öffnen, empfiehlt es sich, diese zunächst auf der Festplatte zu speichern. Um sich deren Inhalt anzeigen zu lassen, reicht ein Viewer aus. Mit einem solchen Programm lässt sich fast jede Datei öffnen, selbst dann, wenn die entsprechende Quellenanwendung nicht auf Ihrem PC installiert ist. Viewer führen keine Makros aus und bieten somit den besten Schutz.

Formularbeginn

/graphics/bild_db	Wer Dokumente n
-------------------	-----------------

Formularende



Wer Dokumente nicht direkt in Office öffnet, sondern stattdessen den Inhalt nur mit einem einfachen Viewer betrachtet, braucht keine Angst vor eingebetteten Makroviren zu haben.

Microsoft etwa stellt für die Office-Applikationen Excel, Word, Powerpoint und Access derartige Gratis-Viewer unter <http://office.microsoft.com/germany/downloads> kostenlos zur Verfügung. Eine sehr gute Alternative stellt ein universeller Dateibetrachter wie Quick View Plus 7.0 dar, der über 250 Dateiformate darstellen kann.

Den deutschen Vertrieb hat die Firma Softline übernommen, die unter [www.softline.de](http://www.softline.de) eine für normale Office-Anwendungen voll taugliche 30-Tage-Demoversion anbietet. Die Vollversion kostet 49 Euro. Allerdings: Damit Sie das Dokument auch bearbeiten können, müssen Sie es in der jeweiligen Anwendung öffnen. Ein Viewer ermöglicht nur eine Vorauswahl in Sachen Vertrauenswürdigkeit, und Sie gehen dann beim Öffnen immer noch ein Risiko ein.

### **Drei-Klassen-Gesellschaft: Nicht jeder darf alles**

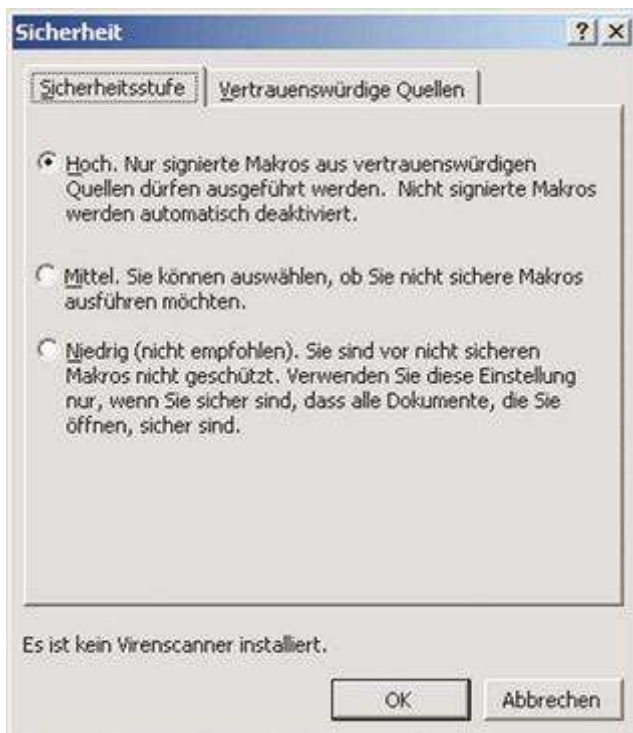
Wer dennoch die Daten in die Office-Anwendung laden will oder muss, sollte auf jeden Fall die Makro-Sicherheitseinstellungen überprüfen, die es seit Office 2000 für Word, Excel, Powerpoint und Outlook gibt.

Unter "Extras, Makro, Sicherheit" stehen in jeder der vier Anwendungen drei Stufen zur Auswahl, die festlegen, ob und welche Makros ausgeführt werden. Zur Klassifizierung dienen digitale Signaturen, die den Urheber der Makros identifizieren und gewährleisten, dass kein Unbefugter den Code verändert hat.

Formularbeginn

/graphics/bild_db	Ab Office 2000 g
-------------------	------------------

Formularende



[Ab Office 2000 gibt es Makro-Sicherheitseinstellungen mit einer dreistufigen Auswahl.](#)

Die - sinnvolle - Standardeinstellung lautet "Hoch" und deaktiviert sämtliche unsignierten Makros. Wenn Sie ein Dokument öffnen, das Makros enthält, erscheint jedoch zunächst kein Hinweis darauf - den gibt es erst dann, wenn ein Makro ausgeführt werden soll.

Word etwa blockierte im Test Makroviren zuverlässig. Allerdings gibt das Programm jedes Mal, wenn ein unsigniertes Makro ausgeführt werden soll, einen Hinweis - egal, ob es sich um Virencode oder harmlose Anwendermakros handelt. Damit steht zu befürchten, dass diese Warnung, ähnlich wie unter Office 97, manchem Anwender derart lästig wird, dass er die Sicherheit auf die niedrige Stufe stellt, um ungestört arbeiten zu können.

Aber selbst die hohe Sicherheitsstufe bietet Ihnen keinen hundertprozentigen Schutz. Mit den Sicherheitsstufen hat Microsoft in Office digitale Signaturen für VBA-Makros eingeführt. Mit einem solchen Gütesiegel versehene Makros lassen sich auch auf der obersten Sicherheitsstufe ausführen - ohne Hinweis an den Anwender.

Nur wenn der Urheber der Signatur nicht als "vertrauenswürdige Quelle" bekannt ist, fragt Office nach: Wählt der Anwender dann die Option "Makros aus dieser Quelle immer vertrauen" und aktiviert ein Makro, werden signierte Makros dieser Herkunft künftig ohne Rückfrage gestartet. Die digitale Signatur ist nach derzeitigem Wissensstand nicht zu fälschen, allerdings könnte ein Angreifer versuchen, sich einen fremden Schlüssel anzueignen.

### **Design-Fehler: Die Schwachstellen im Konzept**

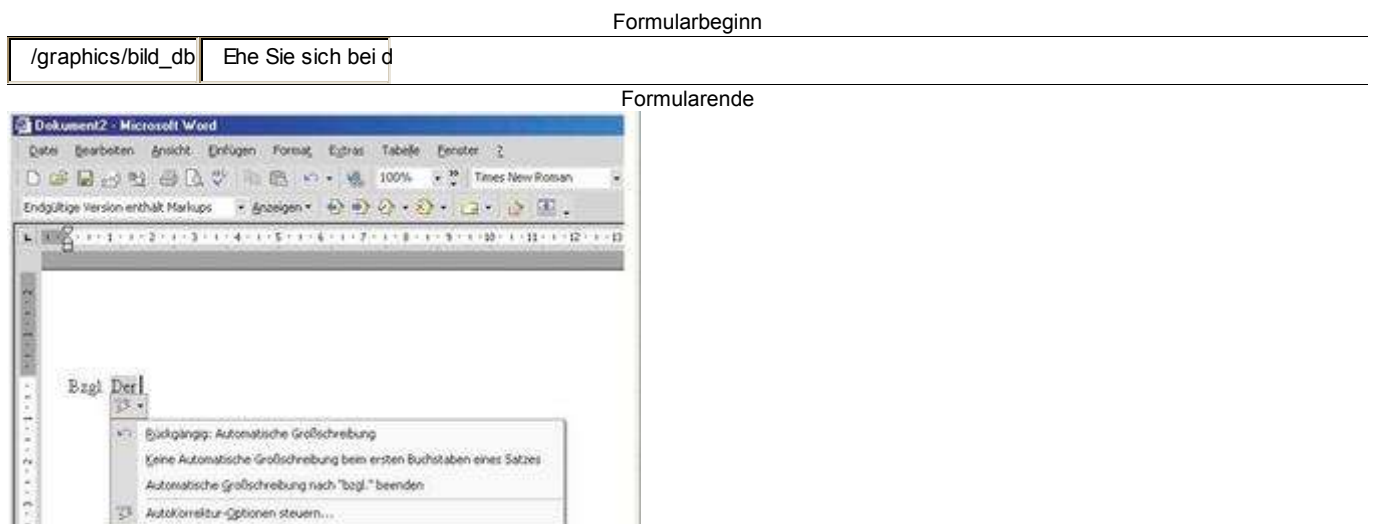
Die mittlere Sicherheitseinstellung entspricht dem bereits von Office 97 bekannten, unzulänglichen Virenschutz: Bei jedem Makro - auch bei völlig harmlosen - erscheint eine Warnung. Der Anwender kann dann das Makro deaktivieren oder das Öffnen des Dokuments abbrechen.

Je mehr makrobewehrte Dokumente ein Anwender bearbeitet, desto schneller nerven die dauernden Warnhinweise - bis er sie möglicherweise abschaltet, um seine Ruhe zu haben. Die niedrigste Sicherheitsstufe schließlich erlaubt die Ausführung aller Makros, ungeachtet der Quelle, aus der sie stammen.

Richtig durchdacht hat Microsoft das Konzept allerdings nicht, denn es weist einen erheblichen Design-Fehler auf: Aus dem Vorlagenverzeichnis, das Sie unter "Extras, Optionen" auf der Registerkarte "Speicherort für Dateien" einstellen, öffnet Office Dokumente mit Makros auf jeder Sicherheitsstufe ohne Warnung. Ein weiteres Manko: Microsoft hat es versäumt, den Virenschutz unter Access zu implementieren. Hier kann ein Makrovirus also völlig ungehindert eindringen.

### Smart Tags: Risiko durch ausführbaren Code

Ein weiteres Sicherheitsrisiko sind die Smart Tags, die als Neuerung in Office XP Einzug gehalten haben. Mit Hilfe dieses Features können Entwickler Plug-in-Module erstellen, die Daten in Office-Dokumenten erkennen und XML-basierte (Extensible Markup Language) Eigenschaftsinfos hinzufügen.



[Ehe Sie sich bei der Textbearbeitung von Smart Tags helfen lassen, sollten Sie mit einem Virens Scanner sichergestellt haben, dass diese keine eingebetteten Viren enthalten.](#)

Bei solchen Plug-ins handelt es sich um ausführbaren Code, es stellt sich also sofort die Frage: Wie steht es mit der Sicherheit? Schließlich kann niemand im Voraus erkennen, was genau sich hinter einem interessant klingenden Eigenschaftsdialog verbirgt.

### Kontrolle über Smart Tags

Eine gewisse Kontrolle über Smart Tags erlaubt Microsoft dem Anwender mit den gleichen Mechanismen, die auch für Makros greifen. Die in "Extras, Makro, Sicherheit" getroffenen Einstellungen entscheiden also darüber, wie Smart Tags behandelt werden.

Wenn die Makro-Sicherheitsstufe für eine Anwendung auf "Hoch" eingestellt ist, werden nicht signierte Smart-Tag-Plug-ins nicht geladen. Entwickler von Smart Tags können diese digital signieren lassen, so dass sie auch bei hoher Makrosicherheit verwendet werden können. Ist die Sicherheitsstufe auf "Mittel" eingestellt, weist eine Warnmeldung den Anwender darauf hin, dass das Programm zum Laden von nicht signiertem Code aufgefordert wird.


Sehr problematisch ist unseres Erachtens allerdings, dass die Standardeinstellung ("Allen installierten Add-ins und Vorlagen vertrauen" im Menü "Extras, Makro, Sicherheit", Registerkarte "Vertrauenswürdige Quellen") jeden Smart Tag ohne Beachtung der Sicherheitsstufe zulässt. Bei Makros gilt dies nicht.

### Schützenswert: Die globale Vorlage

In Word ab Version 97 missbrauchen Viren bevorzugt die zentrale Dokumentvorlage, um sich auf dem Computer breit zu machen. Sie sollten ihr daher auch einen besonderen Schutz zukommen lassen. Aktivieren Sie daher zunächst unter "Extras, Optionen, Speichern" die "Automatische Anfrage für

Speicherung von Normal.dot", die in der Voreinstellung abgeschaltet ist. Diese Option lässt sich seit Word 97 vornehmen.

Formularbeginn	
<a href="#">/graphics/bild_db</a>	Schützen Sie die
Formularende	

[Schützen Sie die globale Dokumentvorlage NORMAL.DOT.](#)

Sie sichern damit das Speichern der Standard-Dokumentvorlage durch eine vorausgehende Rückfrage ab. Haben Sie selbst keine Änderung an der NORMAL.DOT vorgenommen - beispielsweise durch eigene Makros oder Änderungen der Formatvorlage -, haben Sie es eventuell mit einem Virus zu tun, der versucht, die Vorlage zu infizieren.

Eine weitere Möglichkeit, die Datei NORMAL.DOT vor unbefugten Änderungen zu schützen, finden Sie im Visual-Basic- Editor, zu dem Sie über "Alt"- "F11" gelangen. Wechseln Sie dort über "Ansicht, Projekt-Explorer" zum Explorer-Fenster, klicken Sie auf den Eintrag "Normal", und rufen Sie mit der rechten Maustaste den Dialog "Eigenschaften von Normal" auf.

Auf der Registerkarte "Schutz" aktivieren Sie die Option "Projekt für die Anzeige sperren" und vergeben zum Abschluss ein Kennwort. Jeder, der die NORMAL. DOT ändern will, muss von jetzt an dieses Passwort eingeben.

### **Nicht ganz ohne: VBA loswerden**

Viele Makroviren sind allerdings in der Lage, die vorher in den Konfigurationstipps dargestellten Schutzmaßnahmen zu umgehen. Angesichts dessen und auch mit Blick auf die Defizite der integrierten Verteidigungsmechanismen dürfte sich mancher Anwender die Frage stellen, ob es nicht besser sei, ganz auf VBA zu verzichten.

Diese Radikalkur können Sie bereits bei der benutzerdefinierten Installation von Office durchführen, indem Sie aus den gemeinsam genutzten Komponenten das Modul "Visual Basic für Applikationen" abwählen.

Formularbeginn	
<a href="#">/graphics/bild_db</a>	Wer Visual Basic
Formularende	



Wer Visual Basic für Applikationen -kurz VBA- nicht installiert oder aus Sicherheitsgründen wieder deinstalliert, muss auf den Einsatz der Office-Datenbank Access verzichten.

Auch nachträglich lässt sich die Programmiersprache entfernen. Wählen Sie hierzu in Windows unter "Systemsteuerung, Software, Programme ändern oder entfernen" das Microsoft-Office-Paket aus, und klicken Sie auf "Ändern". Danach deaktivieren Sie wie im vorigen Schritt beschrieben VBA.

Wenn Sie VBA deaktiviert haben, müssen Sie allerdings auf Access verzichten, denn diese Office-Komponente funktioniert ohne VBA nicht. Auch einige Assistenten und Vorlagen basieren auf Makros, die dann nicht mehr zur Verfügung stehen. Bislang erstellte Dateien gehen dadurch allerdings nicht verloren.

### **Indizienbeweis: Verdächtige Aktivitäten**

Wenn Sie sich trotz aller Vorsicht einen Makrovirus eingefangen haben, erkennen Sie das in der Regel nicht gleich. Denn bevor die Plagegeister durch spektakuläre Aktionen auf sich aufmerksam machen, versuchen sie, sich heimlich, still und leise weiter zu verbreiten.

Da dies meistens über eine Infektion der NORMAL.DOT geschieht, sollten Sie regelmäßig die in der Standardvorlage vorhandenen Makros kontrollieren. Sie rufen dazu das Menü "Extras, Makro, Makros" auf, wählen die NORMAL.DOT aus und suchen in der Liste nach verdächtigen Makros, die nicht von Ihnen selber stammen.

Ist die Funktion zum Makroansehen nicht verfügbar? Dann ist dies ein Indiz für einen Befall. In diesem Fall können Sie lediglich die entsprechende Vorlage löschen und durch eine andere mit dem ursprünglichen Namen ersetzen. Dabei besteht allerdings das Risiko, dass diese Vorlage ebenfalls infiziert ist.

Es empfiehlt sich daher, immer eine definitiv virenfreie Version der Standard-Dokumentvorlage auf einem schreibgeschützten Datenträger zur Verfügung zu haben - am besten sichern Sie diese unmittelbar nach der Installation. Wenn Sie auf verschlüsselte Makros stoßen, ist auch hier das Löschen der Vorlage zu empfehlen.

### **Original und Fälschung: Umdefinierte Befehle**

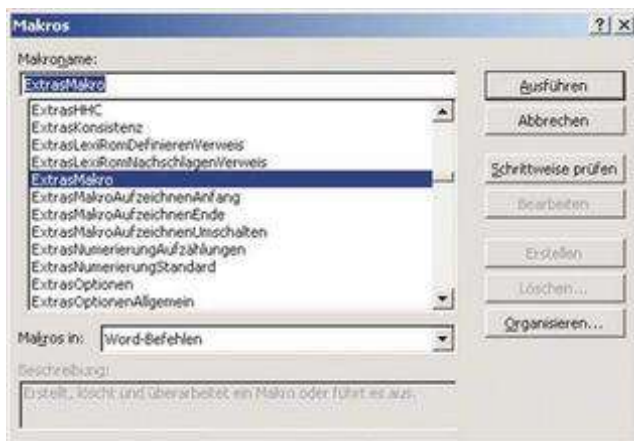
Makroviren sind nicht unbedingt auf die Automakros angewiesen. Beinahe hinter jedem Befehl einer Office-Anwendung steckt ein Makro mit einem bestimmten Namen, das ohne weiteres mit eigenem, anderem Inhalt gefüllt werden kann. Wählt der Anwender einen bestimmten Befehl aus, so wird das Makro dieses Namens - sei es global oder im aktuellen Dokument vorhanden - ausgeführt.

Formularbeginn

/graphics/bild_db	Beinahe jeder Me
-------------------	------------------

Formularende





[Beinahe jeder Menübefehl einer Office-Anwendung besteht aus einem Makro.](#)

Viele Makroviren machen sich dies zunutze und greifen auf bestimmte Befehle zurück, beispielsweise zur Weiterverbreitung oder für die Schadensroutine. Sehr oft verwendete Befehle, brisanterweise aber auch die Befehle "Datei, Dokumentvorlage, Organisieren" und "Extras, Makro", mit denen Sie eigentlich ein Dokument nach Makros untersuchen und löschen können, werden häufig von Viren abgefangen, verändert oder deaktiviert. Auch hier müssen Sie den Virus durch Überschreiben der NORMAL.DOT mit einer unverfälschten Version deaktivieren, um an die Makros heranzukommen.

### **Weitere Hinweise für Virenbefall**

Neben den schon erwähnten Anzeichen für Virenbefall gibt es noch andere Hinweise, die aber weitaus diffuser sind :

- \* Das Laden Ihrer Dokumente dauert wesentlich länger als früher, obwohl Sie am Rechnersystem nichts verändert haben.
- \* Dokumente, die Sie bereits auf korrekte Rechtschreibung geprüft haben, weisen plötzlich wieder Schreibfehler auf, beispielsweise Buchstabendreher.
- \* Der freie Festplattenplatz auf Ihrem System nimmt schnell ab, obwohl Sie keine neuen Programme installiert haben.
- \* Ungewöhnliche Festplattenaktivitäten sind zu bemerken: Das Laufwerk arbeitet wie wild, selbst wenn Sie nichts speichern oder laden.
- \* Datei-Attribute wie Größe oder Datum Ihrer Dokumente ändern sich grundlos.
- \* Es treten häufige Programmabstürze oder unerklärliche Fehlermeldungen auf.

### **Zusammenspiel: Schnittstelle für Virens Scanner in Office**

Nicht jede Fehlermeldung weist gleich auf einen Virus hin. Die Frage, ob sich auf Ihrem PC ungebetene Gäste eingeschlichen haben, kann Ihnen nur ein aktueller Virens Scanner eindeutig beantworten. Viren ohne ein solches Tool aufzuspüren und zu beseitigen ist ein unsicheres Unterfangen - schließlich wissen Sie nicht, welche Systemteile bereits verseucht sind.

Microsoft hat in Office eine Schnittstelle für andere Software-Hersteller integriert, so dass sich deren Virenschutzprodukte in Office einklinken können. Dadurch lassen sich Dokumente zwischen der

Anforderung durch eine Office-Anwendung und dem Öffnen des Dokuments untersuchen. Stellt der Scanner dabei einen Virus fest, erhält der Benutzer eine Meldung, bevor die Datei ohne die befallenen Makros angezeigt wird.

Ob Antiviren-Programm und Office zusammenarbeiten, sehen Sie seit der Version 2000 unter "Extras, Makro, Sicherheit" im unteren Teil des Dialogfeldes. Wenn es dort heißt "Es ist kein Virens Scanner installiert" bedeutet dies lediglich, dass Ihr Scanner die Antiviren-Schnittstelle von Microsoft nicht bedient.

### **Die Kombination macht's: Nur Bordmittel reichen nicht**

Wie Sie gesehen haben, reichen die Bordmittel von Office im Kampf gegen Viren nicht aus. Dazu lassen sich die Schutzeinstellungen, die Sie innerhalb der Programme vornehmen, von den Schädlingen zu einfach austricksen. Hinzu kommen konzeptionelle Mängel, etwa bei der Makrosicherheit.

Doch auch ein Virens Scanner bietet keinen hundertprozentigen Schutz vor Makroviren: Schließlich kann er meist nur auf Viren reagieren, die bekannt sind, denn heuristische Verfahren arbeiten bei Makroviren nicht zuverlässig. Um Ihr System so gut wie möglich zu schützen, sollten Sie daher sowohl eine Antiviren-Software einsetzen als auch die dargestellten Konfigurationsmöglichkeiten nutzen.