Makros in *Office*-Paketen deaktivieren

1 Vorwort

Office-Programme (Outlook, Word, Excel, PowerPoint, Access, Publisher, …) erlauben eine automatisierte Verarbeitung bestimmter Vorgänge mit Hilfe von sogenannten *Makros*. **Makros können auch von Schad-Software (Viren, Trojaner, …) benutzt werden, um Dateien zu verändern, zu löschen oder zu verschlüsseln.** Verschlüsselungs-*Trojaner* tarnen sich beispielsweise in *Office*-Dokumenten für Bewerbungen auf Stellenanzeigen. Die Bewerbung nimmt dabei häufig Bezug auf eine tatsächliche Stellenausschreibung, sodass man quasi gezwungen ist, die Dokumente zu öffnen, wenn man Näheres zu den Bewerbern erfahren will. Abhängig von den Einstellungen der *Office*-Programme werden die *Makros* mit Schad-Software in der Regel sofort oder nach Rückfrage und Bestätigung durch die bearbeitende Person ausgeführt.

Da die meisten Personen der Hochschule Fulda nie oder selten *Makros* bei ihrer Arbeit benötigen, sollten *Office*-Pakete so konfiguriert werden, dass ***Makros* generell nicht ausgeführt werden**, damit Schäden durch Schad-Software soweit wie möglich vermieden werden. Falls *Makros* wider Erwarten regelmäßig für die tägliche Arbeit benötigt werden, sollte die Einstellung so vorgenommen werden, dass man die Ausführung eines *Makros* bestätigen muss, bevor es ausgeführt wird.

Jeder kann sehr einfach verhindern, dass *Makros* automatisch ausgeführt werden. Haben Sie bitte Verständnis dafür, dass Sie die Einstellungen selbst vornehmen müssen, da die PC-Administratoren bzw. PC-Administratorinnen oder der *Helpdesk* die *Office*-Pakete aller Rechner aus Zeitgründen nicht einstellen können. Dieses Dokument beschreibt, welche Einstellungen Sie bei den verschiedenen *Office*-Versionen vornehmen müssen. Falls Sie trotzdem Fragen haben, wenden Sie sich bitte an Ihre(n) PC-Administrator(in) bzw. den *Helpdesk* des Rechenzentrums.

Stimmen Sie niemals der Ausführung eines *Makros* (Anfrage: „Inhalt aktivieren“) oder irgendeiner anderen Aktion zu, wenn Sie ein *Office*-Dokument per *E-Mail* erhalten haben. Sie könnten zum Beispiel folgende Meldung sehen, wenn Sie ein derartiges Dokument öffnen: *Dieses Dokument wurde mit einer älteren Version von Microsoft Word erstellt. Um den Kompatibilitätsmodus zu aktivieren, klicken Sie auf „Bearbeitung aktivieren“ und anschließend auf „Inhalt aktivieren“ in der Leiste oberhalb dieses Dokuments*. Falls Sie auf „Inhalt aktivieren“ klicken, haben Sie Makros aktiviert und Ihr Rechner kann infiziert werden. **Denken Sie immer daran, dass Ihnen *normale* Dokumente keine Fragen stellen und Sie auch zu nichts auffordern, wenn Sie sie mit einem *Office*-Programm öffnen.** Informieren Sie bitte **umgehend** den IT-Sicherheitsbeauftragten bzw. die IT-Sicherheitsbeauftragte Ihrer Organisationseinheit **und** den IT-Sicherheitsbeauftragten bzw. die IT-Sicherheitsbeauftragte des Rechenzentrums **und** die für *E-Mail* zuständige Person im Rechenzentrum oder den *Helpdesk* des Rechenzentrums, wenn Sie so ein Dokument per *E-Mail* erhalten haben. Sie finden die Namen, Telefonnummern und *E-Mail*-Adressen auf der Web-Seite der Hochschule Fulda zur IT-Sicherheit (https://www.hs-fulda.de/it-sicherheit) im Abschnitt „Ansprechpartner“. Falls die *E-Mail* eine Postadresse enthält, können Sie die angehängten Unterlagen als Papierdokumente per Post anfordern.

Wenn Sie glauben, dass Sie einen *Virus*, einen *Trojaner* oder eine andere Schad-Software aktiviert haben, muss das betroffene System so schnell wie möglich vom Hochschulnetz getrennt werden, um weitere Schäden durch Verbreitung der Schad-Software auf andere Systeme zu vermeiden. Das betroffene System sollte **möglichst nicht vom Stromnetz getrennt** und auch **nicht heruntergefahren werden**, damit ggf. später forensische Analysen durchgeführt werden können, um die Schad-Software und die verursachten Schäden zu untersuchen und danach Maßnahmen zur Eindämmung von Folgeschäden getroffen werden können.

- Wenn der Rechner mit einem **Netzwerkkabel** mit dem Hochschulnetz verbunden ist, sollte das Kabel abgezogen werden. Das Kabel ist mit einem Häkchen versehen, das manchmal unter einer Plastikabdeckung versteckt ist und vor dem Abziehen heruntergedrückt werden muss.
- Wenn der Rechner über das **Funknetz (WLAN)** mit dem Hochschulnetz verbunden ist, sollten Sie versuchen, das Netz über den WLAN-Schalter oder den berührungssensitiven Bildschirm (*Touchscreen*) auszuschalten. Falls die Schad-Software dies verhindert, sollten Sie versuchen, das Gerät auszuschalten, indem Sie den Ein-/Ausschaltknopf mehrere Sekunden herunterdrücken. Trennen Sie in diesem Fall das Gerät auch vom Stromnetz, falls es damit verbunden ist und entfernen Sie die Batterie, falls dies möglich ist.

Informieren Sie danach bitte sofort den *Helpdesk* des Rechenzentrums und die Person, die für die Administration des Rechners zuständig ist.

Erstellen Sie regelmäßig (täglich) Sicherungskopien (*Backup*) von allen wichtigen Dateien Ihres lokalen Rechners, damit Sie die Dateien wiederherstellen können, wenn sie doch einmal von einem Verschlüsselungs-*Trojaner* verschlüsselt worden sind. **Der Datenträger für die Sicherungskopie darf nur für die Dauer der Datensicherung am Rechner angeschlossen sein**, damit er nicht ebenfalls verschlüsselt wird, wenn ein Verschlüsselungs-*Trojaner* sein Unwesen treibt. Zahlen Sie niemals Lösegeld für einen Schlüssel zum Entschlüsseln der Dateien, da Sie in der Regel keine Gegenleistung für Ihr Geld erhalten. **Lassen Sie die Software eines infizierten Rechners immer neu installieren und alle Daten von der Sicherungskopie wiederherstellen**, da Sie sonst nicht sicher sein können, dass die Schad-Software vollständig entfernt worden ist.

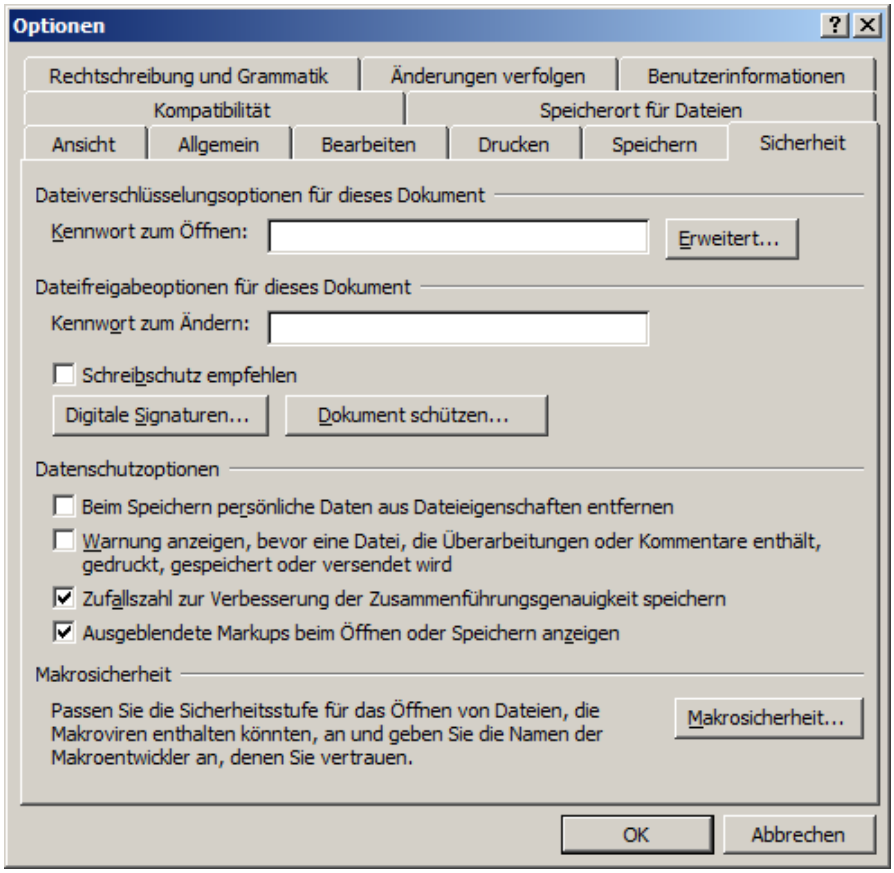
Leider gibt es für „*Microsoft Office*“-Produkte **keine globale Einstellung**, sodass die Einstellungen **nacheinander für jedes Office-Produkt** (Outlook, Word, Excel, Power Point, Access, Publisher, …) individuell vorgenommen werden müssen. Die Bildschirmfotos wurden mit den verschiedenen Versionen der Textverarbeitung *Word* gemacht.

Bitte überprüfen Sie regelmäßig (einmal im Monat) und spätestens nach einem *Office-Update*, dass die Einstellungen nicht wieder automatisch ohne Ihr Wissen auf die Standardeinstellungen geändert worden sind. Da Microsoft jeden zweiten Dienstag eines Monats *Updates* zur Verfügung stellt und ggf. auch automatisch installiert, sollten Sie danach die Einstellungen überprüfen.

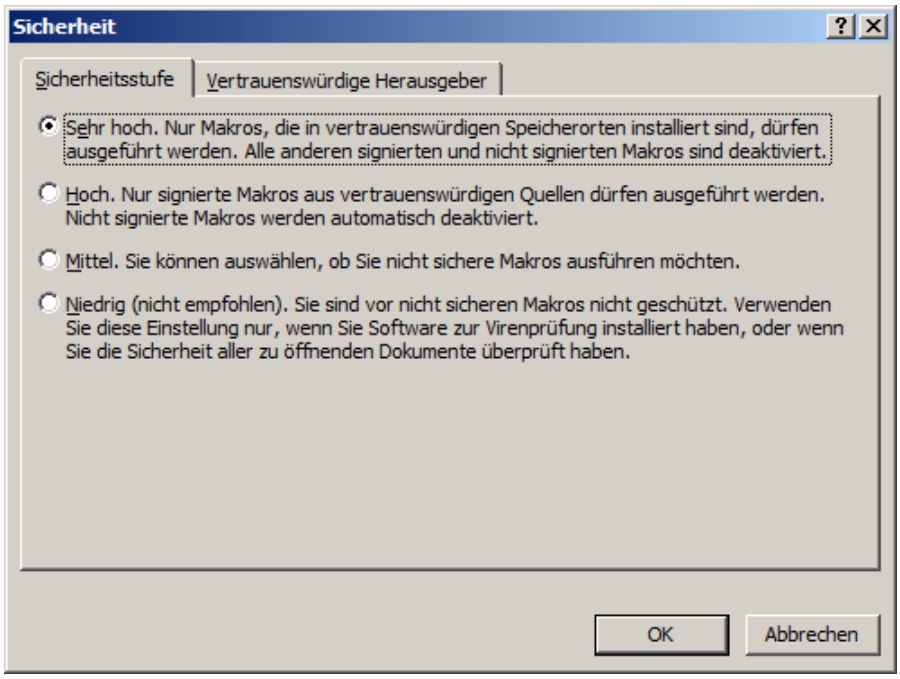
In den Einstellungshinweisen ab Kapitel 2 bedeutet "Extras > ... > ...", dass Sie im entsprechenden Eintrag der Menüzeile am oberen Rand des Programmfensters beginnen (z. B. "Extras") und dann mit einem Eintrag des Menüs, einem Karteikartenreiter oder einem anderen Element weitermachen, das die entsprechende Beschriftung aufweist.

2 Microsoft Office 2003

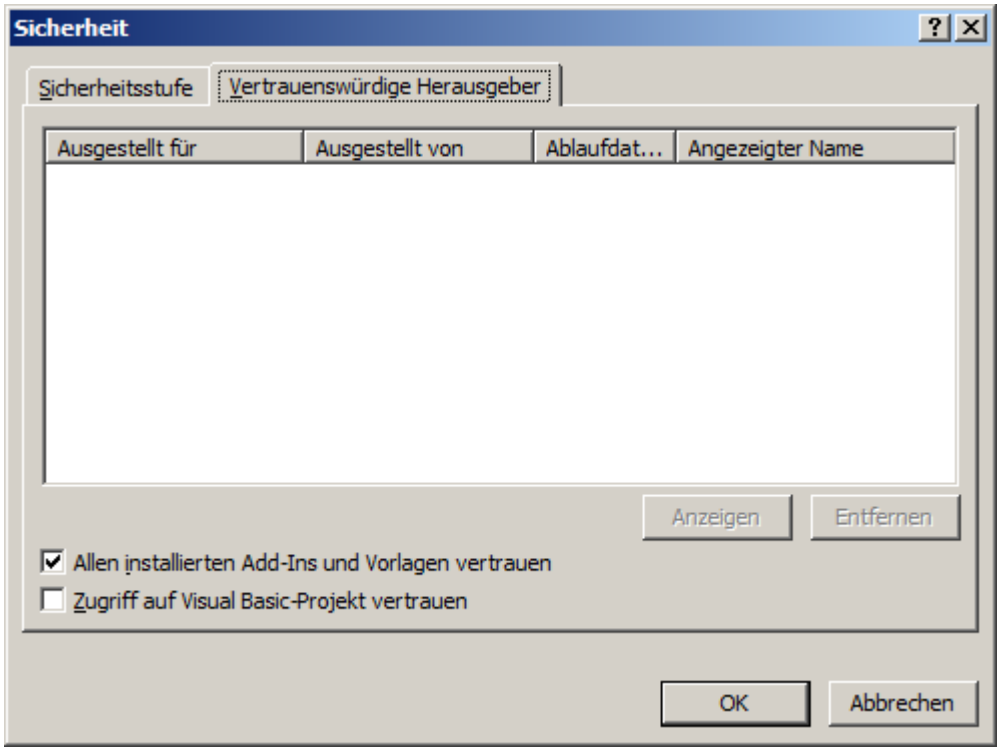
Klicken Sie auf „Extras > Optionen…“, um das Optionen-Menü zu öffnen.



Wählen Sie den Reiter „Sicherheit“ und dann das Feld „Makrosicherheit…“.



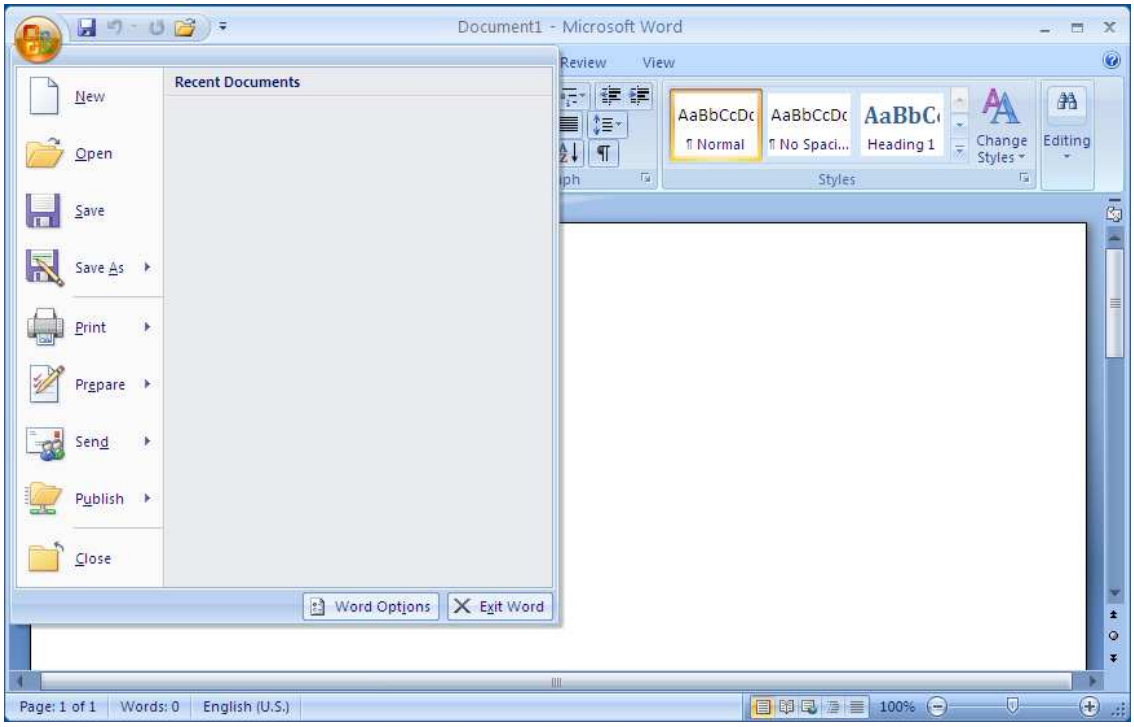
Wählen Sie die Sicherheitsstufe „Sehr hoch. …“ und danach den Reiter „Vertrauenswürdige Herausgeber“ aus.



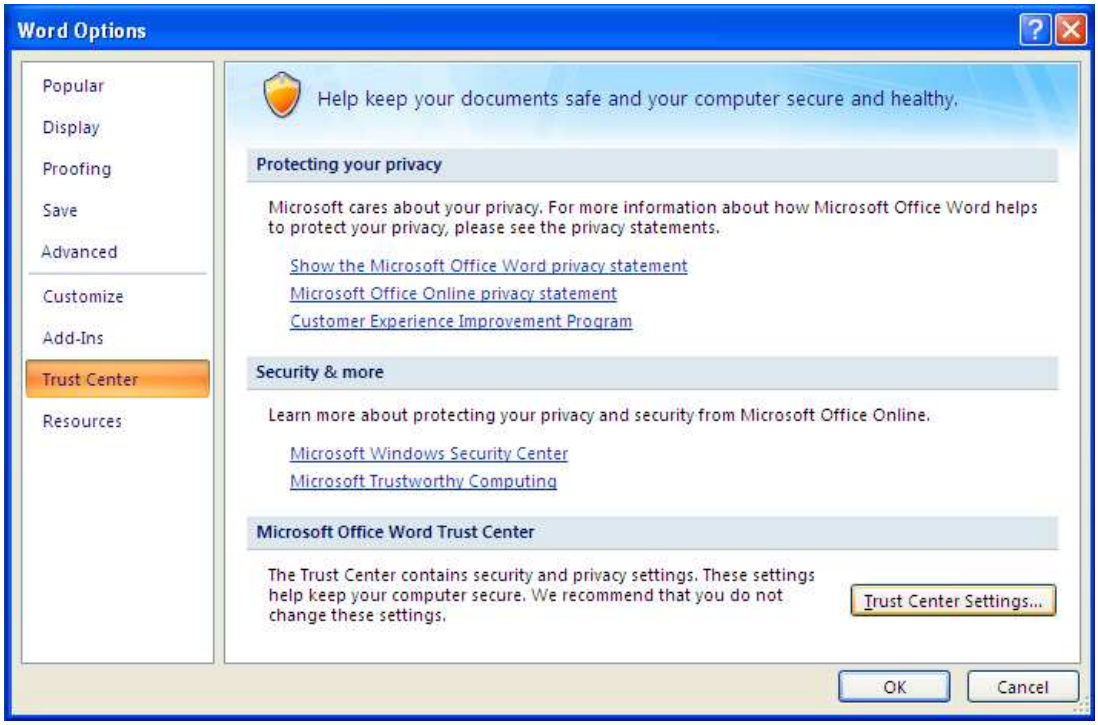
Eventuell kann der Haken vor „Allen installierten Add-Ins und Vorlagen vertrauen“ entfernt werden, um die Sicherheit weiter zu erhöhen. Er darf auf keinen Fall entfernt werden, wenn Sie den *Duden-Korrektor* benutzen, da er dann nicht mehr funktionieren würde.

3 Microsoft Office 2007

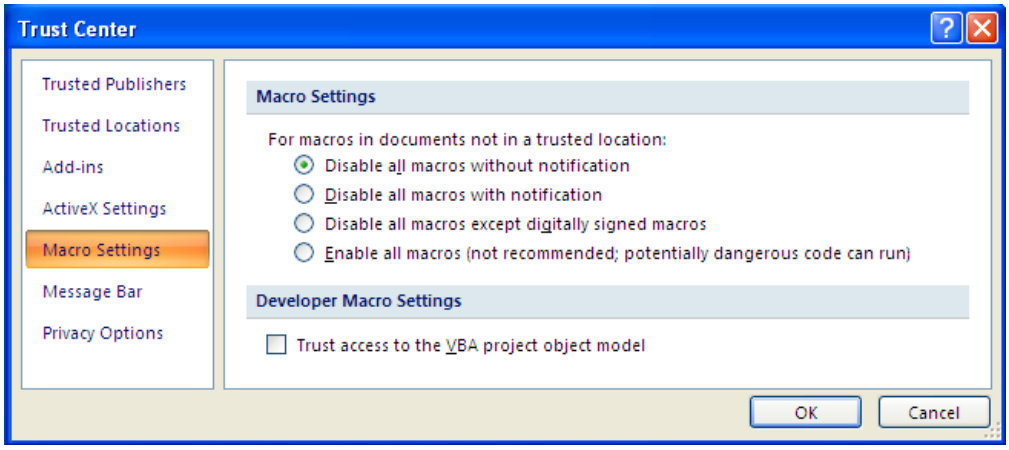
Klicken Sie auf das runde *Windows*-Symbol in der linken oberen Ecke, um ein Menü zu öffnen. Leider habe ich *Office 2007* nur in der englischen Version, sodass Sie in Ihrer Version ggf. entsprechende deutsche Namen verwenden müssen.



Klicken Sie auf „Word Options“, um das Optionen-Menü zu öffnen.



Wählen Sie „Trust Center“ aus und klicken Sie dann auf „Trust Center Settings…“.

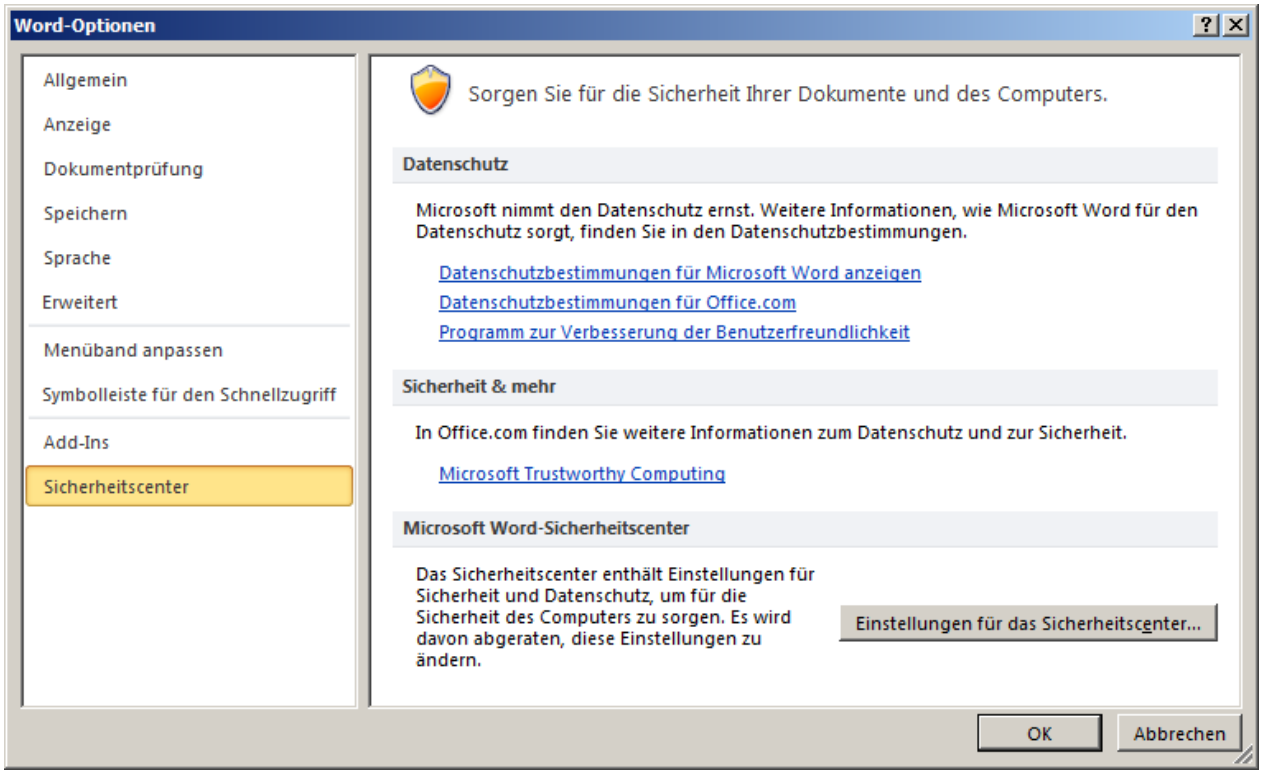


Wählen Sie „Macro Settings“ und dann die Sicherheitsstufe „Disable all macros without notification“ aus. Falls *Makros* in Ihren eigenen Dokumenten doch einmal benötigt werden, kann die Einstellung „Disable all macros with notification“ gewählt werden. In diesem Fall müssen Sie jedes Mal bestätigen, dass ein *Makro* ausgeführt werden darf, bevor es ausgeführt wird. Achten Sie darauf, dass Sie nur Ihre eigenen Makros aktivieren.

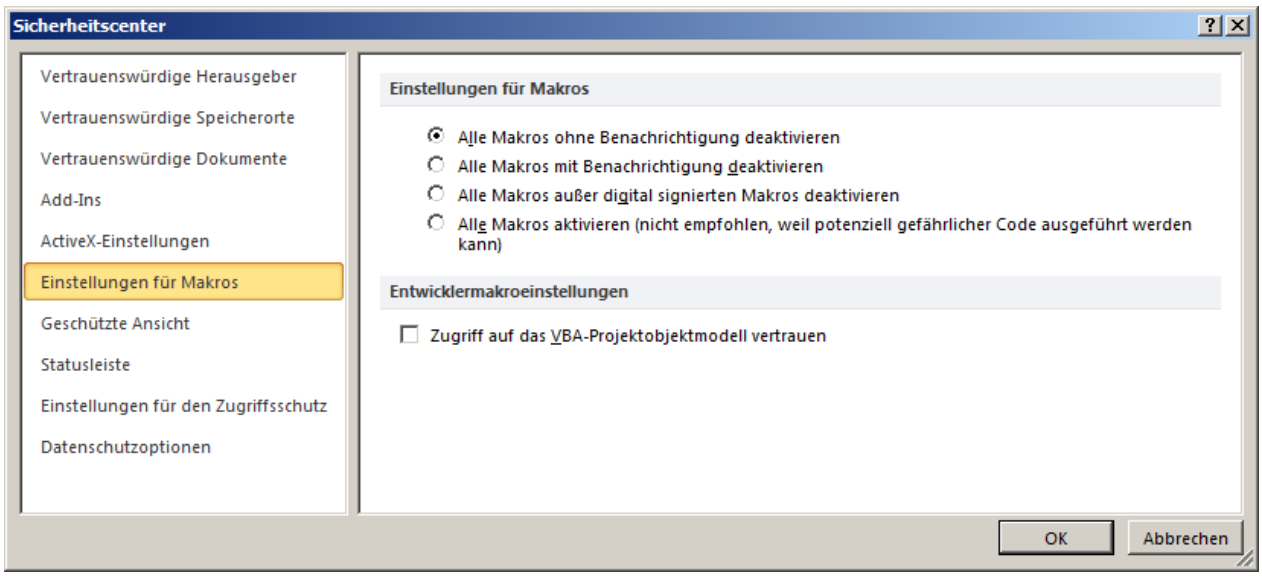
Wählen Sie „ActiveX Settings“ und dann die Sicherheitsstufe „Disable all controls without notification“ aus.

4 Microsoft Office 2010

Klicken Sie auf „Datei > Optionen…“, um das Optionen-Menü zu öffnen.

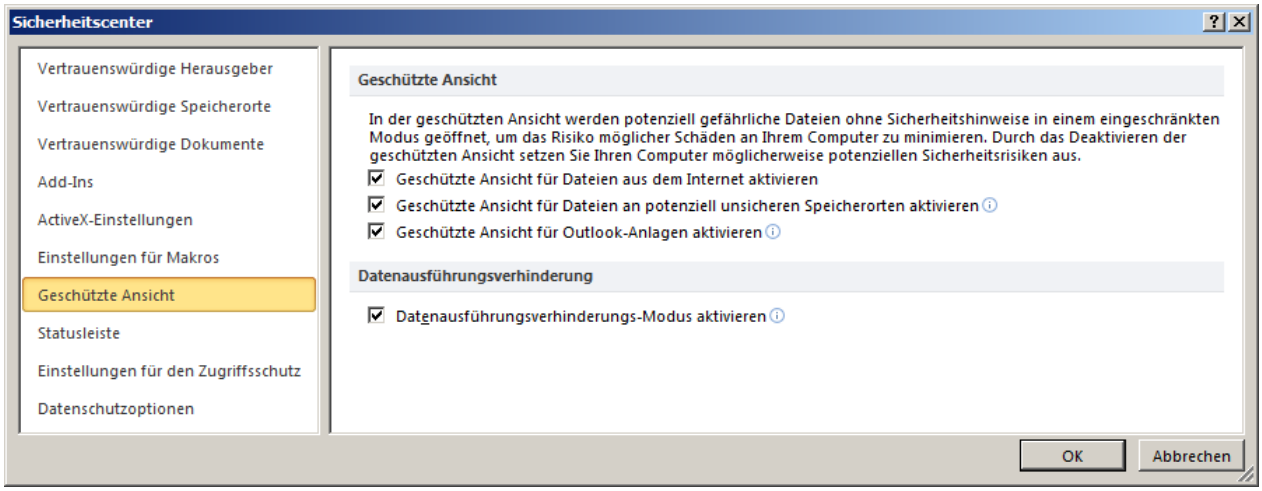


Wählen Sie „Sicherheitscenter“ und dann „Einstellungen für das Sicherheitscenter…“ aus.



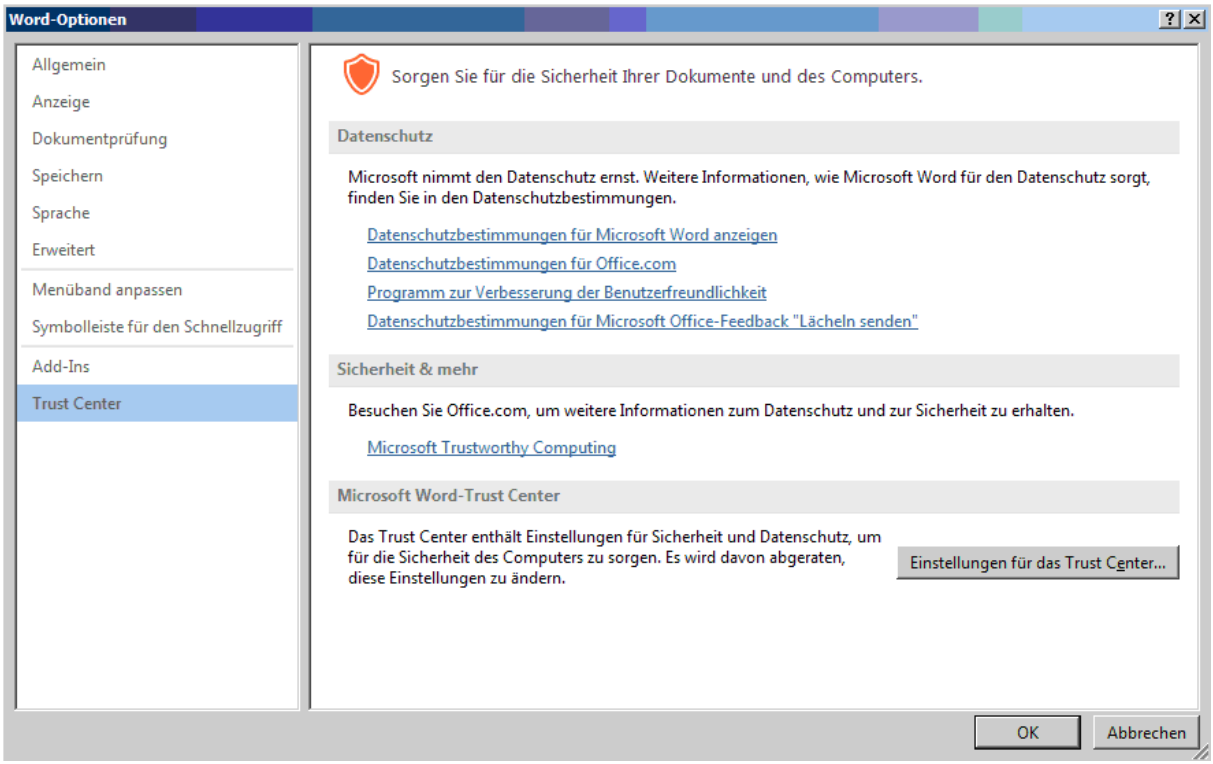
Wählen Sie „Einstellungen für Makros“ und dann „Alle Makros ohne Benachrichtigung deaktivieren“ aus. Falls *Makros* in Ihren eigenen Dokumenten doch einmal benötigt werden, kann die Einstellung „Alle Makros mit Benachrichtigung deaktivieren“ gewählt werden. In diesem Fall müssen Sie jedes Mal bestätigen, dass ein *Makro* ausgeführt werden darf, bevor es ausgeführt wird. Achten Sie darauf, dass Sie nur Ihre eigenen Makros aktivieren.

Wählen Sie „Geschützte Ansicht“ aus, falls es vorhanden ist (fehlt z. B. bei „Outlook“). Alle Einträge sollten einen Haken haben.

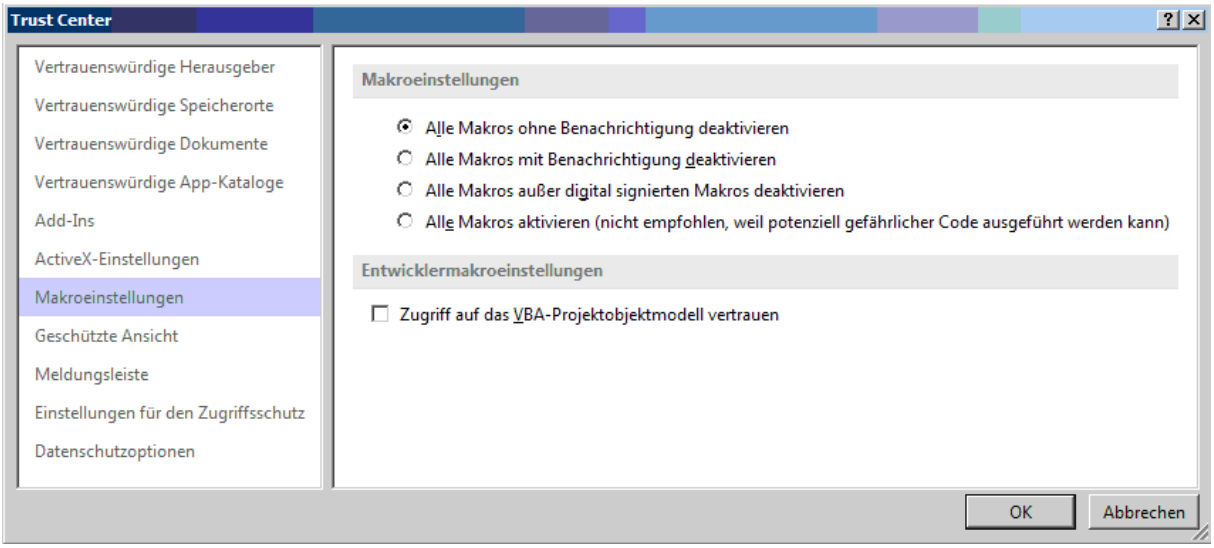


5 Microsoft Office 2013, 2016, 2019 und 365

Das Optionen-Menü wird abhängig von der *Office*-Version und dem gewählten Programm auf verschiedene Arten geöffnet. Klicken Sie auf „Datei“, „Weitere Dokumente öffnen“, „Weitere Arbeitsmappen öffnen“, „Weitere Präsentationen öffnen“ oder „Weitere Publikationen öffnen“ und dann auf „Optionen“, um das Optionen-Menü zu öffnen. Die folgenden Bildschirmfotos stammen von „Word 2013“.

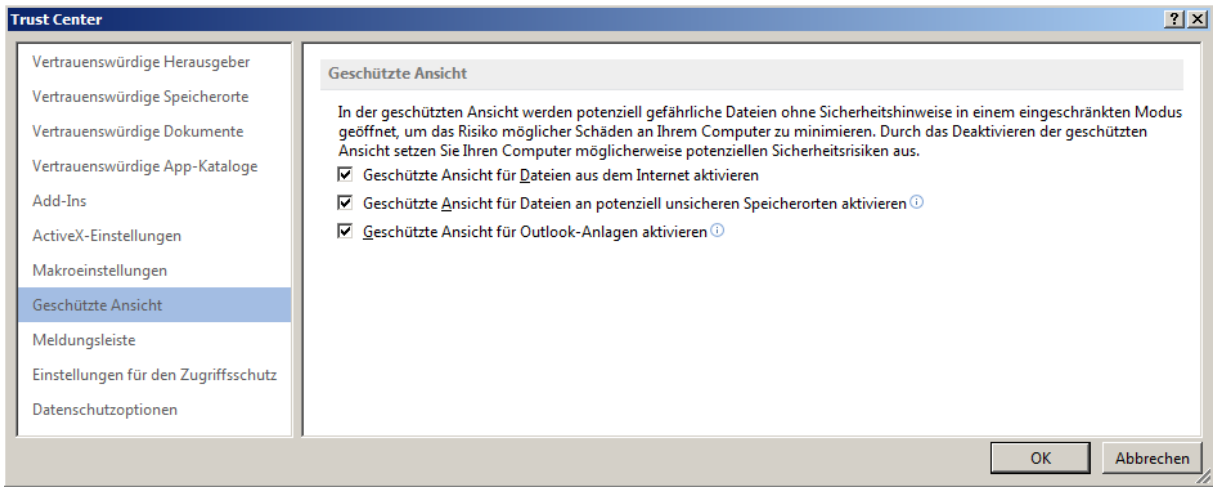


Wählen Sie „Trust Center“ und dann „Einstellungen für das Trust Center…“ aus.



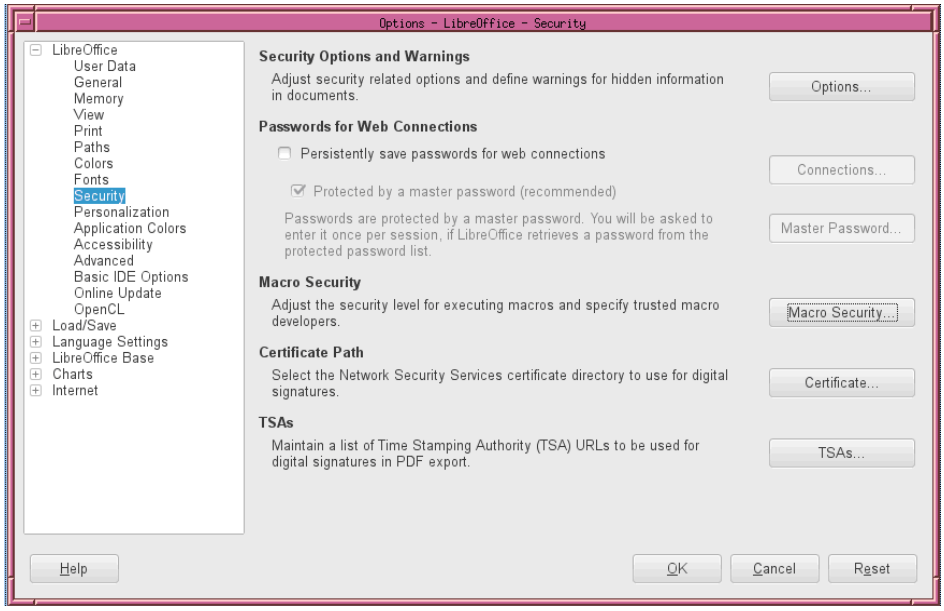
Wählen Sie „Makroeinstellungen“ und dann „Alle Makros ohne Benachrichtigung deaktivieren“ aus. Falls *Makros* in Ihren eigenen Dokumenten doch einmal benötigt werden, kann die Einstellung „Alle Makros mit Benachrichtigung deaktivieren“ gewählt werden. In diesem Fall müssen Sie jedes Mal bestätigen, dass ein *Makro* ausgeführt werden darf, bevor es ausgeführt wird. Achten Sie darauf, dass Sie nur Ihre eigenen Makros aktivieren.

Wählen Sie „Geschützte Ansicht“ aus, falls es vorhanden ist (fehlt z. B. bei „Outlook“). Alle Einträge sollten einen Haken haben.

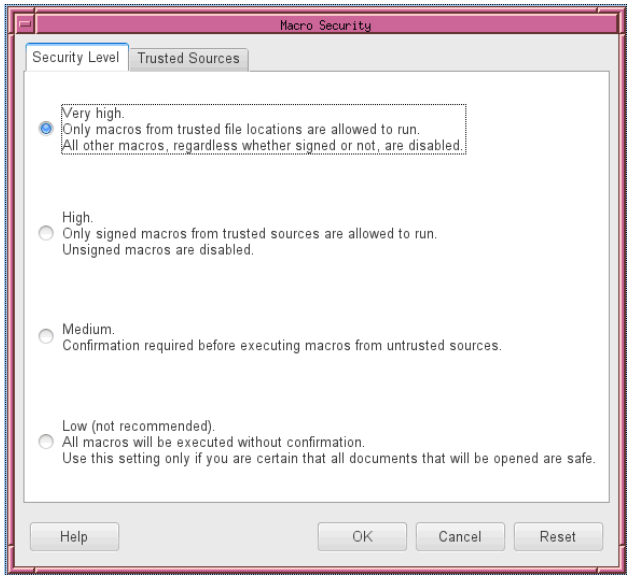


6 LibreOffice 5.x bis 7.x

Klicken Sie auf „Tools > Options“, „Extras > Optionen“ oder drücken Sie die Tastenkombination <Alt-F12>, um das Optionen-Menü zu öffnen. *LibreOffice* benutzt eine globale Einstellung, d. h., Sie müssen die Einstellungen nur einmal für alle Programme vornehmen. Die folgenden Bildschirmfotos stammen von LibreOffice 5.x“.



Wählen Sie „Security“ bzw. „Sicherheit“ und dann das Feld „Macro Security“ bzw. „Makro Sicherheit“ aus.



Wählen Sie die Sicherheitsstufe „Very high.“ bzw. „Sehr hoch.“ aus.

Letzte Änderung: 02. November 2021