**MS** Access-Datenbanken

Benutzerdokumentation

Access-Optionen im Sicherheits- / Trust-Center

# Inhalt

1	Gegenstand dieses Dokuments	2
2	Sicherheitsoptionen in MS Access 2010	3
3	Sicherheitsoptionen in MS Access 2013, 2016 und 2019	7
4	Sicherheitsoptionen in MS Access 2007	11

#### 1 Gegenstand dieses Dokuments

Unzweckmässig gesetzte Sicherheitsoptionen in MS Access können das Arbeiten mit MS Access-Datenbanken behindern oder gar verunmöglichen.

In diesem Dokument werden mittels Screenshots die korrekten Sicherheitsoptionen für das Arbeiten mit MS Access-Datenbanken im Netz *und* im Mehrbenutzerbetrieb für die MS Access-Versionen 2010, 2013 und 2016 sowie 2007 dokumentiert.

Die Sicherheitsoptionen gelten nicht pro Datenbank, sondern pro Benutzer (pro PC, pro Access-Installation).

Sie müssen deshalb auf jedem PC angepasst werden.

#### Anmerkung zu den Sicherheitshinweisen von Microsoft:

Microsoft rät ausdrücklich vom Setzen verschiedener Optionen, wie wir sie empfehlen, ab. Angeblich aus Sicherheitsgründen.

Der Autor hat vor einigen Tagen einen mit Malware verseuchten PC bei einem Kunden (KMU) gereinigt. Aufwand: sieben Stunden. Trotz Firewall und Microsoft-Sicherheitseinstellungen konnte ein böswilliger Russe auf trickreiche Art und Weise die Malware installieren und das Bankkonto unseres Kunden um 6 Tausend Franken erleichtern.

Die Malware wurde weder von namhaften Firewalls und Virenscannern, noch von Microsofts Tool zum Entfernen bösartiger Software noch von Microsofts Sicherheitseinstellungen erkannt und blockiert. Nur mit professionellen Werkzeugen (wie u. a. Malwarebytes) konnte die Schadsoftware identifiziert, lokalisiert und vollständig entfernt werden. Microsofts Sicherheitsoptionen, Sicherheitscenter und UAC (Benutzerkontensteuerung) sind potemkinsche Dörfer ...

Die Sicherheitshinweise von Microsoft können ignoriert werden.

Fragen zu diesem Dokument bzw. zu den Sicherheitseinstellungen bitte an <u>experts@access-experts.ch</u> oder Tel. +41 (0)44 950 05 60.

Und hier geht's weiter:

<u>Sicherheitsoptionen in MS Access 2010</u> für Access-2010-Anwender oder <u>Sicherheitsoptionen in MS Access 2013, 2016 und 2019</u> für Access-2013- bis 2019-Anwender oder <u>Sicherheitsoptionen in MS Access 2007</u> für Access-2007-Anwender.

Welche Version Sie haben, erfahren Sie im Menü Datei, Menüpunkt "Hilfe" (2010) bzw. Menüpunkt "Konto" (2013 / 2016 / 2019).

Access-2007-Anwender haben kein Menü Datei, sie klicken die Office-Schaltfläche und hangeln sich via Optionen zu den "Ressourcen" durch.

# 2 Sicherheitsoptionen in MS Access 2010

#### 1. Schritt: Aufruf der Optionen im Menü Datei:



2. Schritt: Aufruf der Einstellungen für das Sicherheitscenter (Sicherheitsoptionen) im Optionsmenü:



Im Sicherheitscenter werden anschliessend die Optionen in sechs Registern so, wie in den Screenshots vorgegeben, angepasst:



Der Ordnerpfad des Datenbankspeicherorts muss nur dann hinzugefügt werden, wenn Benutzer eingeschränkte Rechte im Netzwerk haben.

:	Sicherheitscenter	? 💌
	Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte Vertrauenswürdige Dokumente Add-Ins	Vertrauenswürdige Dokumente Warnung: Vertrauenswürdige Dokumente werden ohne Sicherheitsabfragen zu Makros, ActiveX-Steuerelementen oder anderen Arten aktiver Inhalte im Dokument geöffnet. Bei einem vertrauenswürdigen Dokument werden Sie beim nächsten Öffnen nicht mehr abgefragt, auch nicht, wenn dem Dokument neuer aktiver Inhalt hinzugefügt wurde oder Änderungen an vorhandenem aktiver inhalt vorgenommen wurden. Daher sollten Sie nur Dokumetnen vertrauen, deren Quelle vertrauenswürdig ist.  Vertrauenswürdigkeit von Dokumenten in einem Netzwerk zulassen
	ActiveX-Einstellungen Einstellungen für Makros DEP-Einstellungen Statusleiste Datenschutzoptionen	Vertrauenswürdige Dokumente deaktivieren           Alle vertrauenswürdigen Dokumente bereinigen, sodass sie nicht mehr vertrauenswürdig sind         Bereinigen

Sicherheitscenter		
Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte	ActiveX-Einstellungen für alle Office-Anwendungen	
Vertrauenswürdige Dokumente	<ul> <li>Alle steuerereinente omre benachtenugung geaktiveren</li> <li>Eingabeaufforderung anzeigen, bevor UFI-Steuerelemente (Unsafe for Initialization) mit zusätzlichen Einschränkungen und SFI-Steuerelemente (Safe for Initialization) mit minimalen Einschränkungen aktiviert werden</li> </ul>	
Add-Ins ActiveX-Einstellungen	<ul> <li>Eingabeaufforderung anzeigen, bevor alle Steuerelemente mit minimalen Einschränkungen aktiviert werden</li> <li>Alle Steuerelemente ohne Einschränkungen und ohne Eingabeaufforderung aktivieren (nicht empfohlen, weil potenziell affehliche Gewarelemente auwardicht userden kännen)     </li> </ul>	
Einstellungen für Makros DEP-Einstellungen	Abgesicherter Modus (beschränkt den Zugriff des Steuerelements auf Ihren Computer)	
Statusleiste		
Datenschutzoptionen		

Sicherheitscenter		2
Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte Vertrauenswürdige Dokumente Add-Ins	Einstellungen für Makros          Alle Makros ohne Benachrichtigung deaktivieren         Alle Makros mit Benachrichtigung geaktivieren         Alle Makros außer digital signierten Makros deaktivieren	
ActiveX-Einstellungen	Alle Makros aktivieren (nicht empfohlen, weil potenziell gefährlicher Code ausgeführt werden kann)	
Einstellungen für Makros		
DEP-Einstellungen		
Statusleiste		
Datenschutzoptionen		

Anmerkung zur Makrosicherheit: werden nicht alle Makros aktiviert, funktionieren die meisten Access-Datenbanken nicht mehr.

Vertrauenswürdige Herausgeber         Vertrauenswürdige Speicherorte         Vertrauenswürdige Dokumente         Add-Ins         ActiveX-Einstellungen         Einstellungen für Makros         DEP-Einstellungen	Sicherheitscenter	8
Statusleiste           Datenschutzoptionen	Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte Vertrauenswürdige Dokumente Add-Ins ActiveX-Einstellungen Einstellungen für Makros DEP-Einstellungen Statusleiste Datenschutzoptionen	Einstellungen der Statusleiste für alle Office-Anwendungen Statusleiste anzeigen  Meldungsleiste in allen Anwendungen anzeigen, wenn aktiver Inhalt, wie z. B. ActiveX-Steuerelemente, gesperrt ist  Informationen zu gesperrtem Inhalt <u>n</u> iemals anzeigen



Abschliessend sind die **Clienteinstellungen** (7. Menüpunkt im Optionsmenü) für den Mehrbenutzerbetrieb (mehrere Benutzer arbeiten gleichzeitig mit der Datenbank) anzupassen:

Access-Optionen		
Allgemein	Weboptionen	•
Aktuelle Datenbank	Erweitert	
Datenblatt	Zuletzt verwendete Datenbank beim Starten von Access öffnen	
Objekt-Designer	Standardöffnungsmodus	
Dokumentprüfung		
Sprache	Standard bei Datensatzsperrung	
Clienteinstellungen	Alle Datensätze	
Menüband annassen	Bearbeiteter Datensatz	
menubunu unpussen	Daten <u>b</u> anken mit Sperrung auf Datensatzebene öffnen	
Symbolleiste für den Schnellzugriff	OLE/DDE- <u>T</u> imeout (s): 30	
Add-Ins	Anzeigeaktualįsierungsintervall (s): 60 🚔	
Sicherheitscenter	Anzahl der Datenaktualisierungsversuche: 2	
	OD <u>B</u> C-Anzeigeaktualisierungsintervall (s): 1'500	
	Datenaktualisierungsintervall (ms): 250 🚔	
	DDE-Vorgänge:	
	DE-Anfragen ignorieren	
	DDE-Aktualisierung zulassen	
	Befehlszeilenargumente:	
	Verschlüsselungsmethode:	
	Legacyverschlusselung verwenden (geeignet für Abwartskompatibilität und Mehrbenutzer-Datenbanken)	=
	Standardverschlusselung verwenden (gro <u>b</u> ere Sicherheit)	
	weitere informationen zur verschlusselung	
	Standarddesign	
	Designdatei: Standarddesign für Office Durchsuchen	-
	ОК	Abbrechen

Standardmässig ist die Standardverschlüsselung aktiviert. Mit der Standardverschlüsselung können mehrere Benutzer *nicht* gleichzeitig mit der Datenbank arbeiten. Für den Mehrbenutzerbetrieb ist deshalb die "Legacyverschlüsselung" anzuwenden.

Clienteinstellungen = Einstellungen pro Benutzer-PC, d. h., auch diese Einstellungen müssen **pro PC** individuell wie oben vorgegeben gesetzt werden.

# 3 Sicherheitsoptionen in MS Access 2013, 2016 und 2019

1. Schritt: Aufruf der Optionen im Menü "Datei":

¢			Menue - Gardenpa
Informationen	Informatic	nen	
Neu	ArtikelDBP		
Öffnen	D: » Projekte » 9 GardenParc »	02 Datenbank	
Speichern	<b>i</b> r	Komprimieren und reparieren Verhindern und beheben Sie Datenbankdateiprobleme, indem Sie	Datenbankeigenschaften anze
Speichern unter	Datenbank komprimieren und reparieren	'Datenbank komprimieren und reparieren' verwenden.	
Drucken			
Schließen	<b>3</b>	Benutzer und Berechtigungen verwalten Verwenden Sie Kennwörter und Berechtigungen dazu, für	
Konto	Benutzer und Berechtigungen *	Einzelpersonen oder Personengruppen den Zugriff auf die Objekte in Ihrer Datenbank zu gestatten oder einzuschränken.	
Optionen			
	Datenbankkennwort festlegen	Datenbankkennwort festlegen Verwenden Sie ein Kennwort, um den Zugriff auf die Datenbank zu beschränken. Dateien, die im Dateiformat von Microsoft Access 2007 oder höher vorliegen, werden verschlüsselt.	

2. Schritt: Aufruf der Einstellungen für das Trust-Center (Sicherheitsoptionen) im Optionsmenü:



Im Trust-Center werden anschliessend die Optionen in sechs Registern so, wie in den Screenshots vorgegeben, angepasst:



Der Ordnerpfad des Datenbankspeicherorts muss nur dann hinzugefügt werden, wenn Benutzer eingeschränkte Rechte im Netzwerk haben.

Vertrauenswürdige Herausgeber         Vertrauenswürdige Speicherorte         Vertrauenswürdige Dokumente         Add-Ins         Add-Ins         ActiveX-Einstellungen         Makroeinstellungen         Meldungsleiste         Datenschutzoptionen    Vertrauenswürdige Dokumente bereinigen, sodass sie nicht mehr vertrauenswürdig sind	Trust Center	?
	Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte Vertrauenswürdige Dokumente Add-Ins ActiveX-Einstellungen Makroeinstellungen Meldungsleiste Datenschutzoptionen	Vertrauenswürdige Dokumente Warnung: Vertrauenswürdige Dokumente werden ohne Sicherheitsnachfragen zu Makros, ActiveX-Steuerelementen oder anderen Arten aktiver Inhalte im Dokument geöffnet. Wurde ein Dokument einmal als vertrauenswürdig eingestuft, werden beim nächsten Öffnen keine Sicherheitsabfragen mehr ausgeführt. Dies gilt auch dann, wenn dem Dokument neuer aktiver Inhalt hinzugefügt wurde oder Änderungen an vorhandenem aktivem Inhalt vorgenommen wurden. Daher sollten Sie nur Dokumenten vertrauen, deren Quelle vertrauenswürdig ist. Vertrauenswürdigkeit von Dokumenten in einem Netzwerk zulassen Vertrauenswürdige Dokumente geaktivieren Alle vertrauenswürdigen Dokumente bereinigen, sodass sie nicht mehr vertrauenswürdig sind Bereinigen

Trust Center	
Vertrauenswürdige Herausgeber	ActiveX-Einstellungen für alle Office-Anwendungen
Vertrauenswürdige Speicherorte	
Vertrauenswürdige Dokumente	Alle steuerelemente onne Benachrichtigung <u>d</u> eaktivieren     Einschauff der Leiter (Unsefe for Leiterlichten) wit zur öbelichen Einschröchungen
Add-Ins	Eingabeaufförderung anzeigen, bevor UFI-Steuereiemente (Unsare för Initialization) mit zusätzlichen Einschränkungen und SFI-Steuerelemente (Safe för Initialization) mit minimalen Einschränkungen aktiviert werden
ActiveX-Einstellungen	Eingabeaufforderung anzeigen, bevor alle Steuerelemente mit minimalen Einschränkungen aktiviert werden
Makroeinstellungen	Alle Steuerelemente ohne Einschränkungen und ohne Eingabeaufforderung aktivieren (nicht empfohlen, weil potenziell gefährliche Steuerelemente ausgeführt werden können)
Meldungsleiste	
Datenschutzoptionen	Abgesicherter Modus (beschränkt den Zugriff des Steuerelements auf Ihren Computer)

rust Center	
Vertrauenswürdige Herausgeber Vertrauenswürdige Speicherorte	Makroeinstellungen
Vertrauenswürdige Dokumente	<ul> <li>Alle Makros ohne Benachrichtigung deaktivieren</li> <li>Alle Makros mit Benachrichtigung deaktivieren</li> </ul>
Add-Ins	Alle Makros außer digital signierten Makros deaktivieren
.ctiveX-Einstellungen	Alle Makros aktivieren (nicht empfohlen, weil potenziell gef
kroeinstellungen	
eldungsleiste	
Datenschutzoptionen	

Anmerkung zur Makrosicherheit: werden nicht alle Makros aktiviert, funktionieren die meisten Access-Datenbanken nicht mehr.



Trust Center	2 💌
Vertrauenswürdige Herausgeber	Datenschutzoptionen
Vertrauenswürdige Speicherorte	☑ Office das <u>H</u> erstellen einer Internetverbindung gestatten ○
Vertrauenswürdige Dokumente	🔲 Regelmäßig eine Datei herunterladen, mit deren Hilfe Systemprobleme bestimmt werden können 🛈
Add-Ins	Senden Sie uns Informationen über Ihre Nutzung und die Leistung von Office-Software, um bei der Verbesserung Ihrer
ActiveX-Einstellungen	Office-Dokumente überorüfen, die von verdächtigen Websites stammen oder dorthin verlinken
Makroeinstellungen	Dem Aufgabenbereich "Recherchieren" das Prüfen auf neue Dienste und deren Installation erlauben
Meldungsleiste	Das Office-Feedbacktool ("Lächeln senden") aktivieren, damit ich Feedback zur Verbesserung von Office senden kann
Datenschutzoptionen	Lesen Sie die Datenschutzbestimmungen.

Abschliessend sind die **Clienteinstellungen** (7. Menüpunkt im Optionsmenü) für den **Mehrbenutzerbetrieb** (mehrere Benutzer arbeiten gleichzeitig mit der Datenbank) anzupassen:

Access-Optionen		? 🗙
Allgemein	Erweitert	*
Aktuelle Datenbank	Zuletzt verwendete Datenbank beim Starten von Access öffnen	
Datenblatt	Standardöffnungsmodus	
Objekt-Designer	Freigegeben	
Dokumentprüfung	Standard bei Datensatzsperrung	
Sprache	Keine Sperren	
Clienteinstellungen	Alle Datensätze     Rearbeiteter Datensatz	
Menüband anpassen	Datenbanken mit Sperrung auf Datensatzebene öffnen	
Symbolleiste für den Schnellzugriff	OLE/DDE- <u>Ti</u> meout (s): 30	
Add-Ins	Anzeigeaktualisierungsintervall (s): 60 🔭	
Trust Center	Anzahl der Datenaktualisierungsversuche: 2	
	OD <u>B</u> C-Anzeigeaktualisierungsintervall (s): 1'500	
	Date <u>n</u> aktualisierungsintervall (ms):	
	DDE-Vorgänge:	
	DDE-Antragen ignorieren	
	Befehlszeilenargumente:	
	Verschlüsselungsmethode:	
	Legacyverschlüsselung verwenden (geeignet für Abwärtskompatibilität und Mehrbenutzer-Datenbanken)	
	Standardverschlüsselung verwenden (größere Sicherheit)	=
	Weitere Informationen zur Verschlüsselung	
	Standarddesign	
	Designdatei: Standarddesign für Office Durchsuchen	
	ОК	Abbrechen

Standardmässig ist die Standardverschlüsselung aktiviert. Mit der Standardverschlüsselung können mehrere Benutzer *nicht* gleichzeitig mit der Datenbank arbeiten. Für den Mehrbenutzerbetrieb ist deshalb die "Legacyverschlüsselung" anzuwenden.

Clienteinstellungen = Einstellungen pro Benutzer-PC, d. h., auch diese Einstellungen müssen **pro PC** individuell wie oben vorgegeben gesetzt werden.

# 4 Sicherheitsoptionen in MS Access 2007

In Access 2007 finden Sie die Sicherheitsoptionen so:

1. Office-Schaltfläche

2. Access-Optionen

3. Vertrauensstellungscenter ⇔ Einstellungen für das Vertrauensstellungscenter.

Die Einstellungen der Sicherheitsoptionen können Sie aus den Screenshots für die Sicherheitsoptionen in MS Access 2010 übernehmen. Die Vorgabe der Verschlüsselungsmethode entfällt in Access 2007.

Autor: Rainer Bauer

= Ende des Dokuments =