



## EMPFEHLUNG: IT IN UNTERNEHMEN

# Sichere Konfiguration von Microsoft Word 2013/2016/2019

## für den Einsatz auf dem Betriebssystem Microsoft Windows

Büroanwendungen gehören in Organisationen jeder Größenordnung zu den am häufigsten genutzten Anwendungsprogrammen. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen. Wegen der großen Verbreitung und Angriffsfläche von Office-Produkten werden diese häufig als Angriffsweg genutzt, beispielsweise um mittels Makros in Office-Dokumenten Schadsoftware zu verbreiten und auf Zielsystemen auszuführen. Mit einer wohlüberlegten Konfiguration dieser Produkte kann das Risiko der Ausnutzung von Standardfunktionen oder Schwachstellen minimiert werden.

### Ziel

Hauptaugenmerk dieser Empfehlung liegt auf dem Einsatz von Microsoft Word 2013/2016/2019 in mittelgroßen bis großen Organisationen, in denen die Endsysteme mit Gruppenrichtlinien in einer Active Directory-Umgebung verwaltet werden. Alternativ können diese auch als lokale Sicherheitsrichtlinien angewendet werden.

Bei den vorliegenden 61 Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft Word 2013/2016/2019, die sicherheitsrelevant sind. Weitere Einstellungen finden sich in den BSI-Veröffentlichungen:

- ✓ Sichere Konfiguration von Microsoft Access 2013/2016/2019
- ✓ Sichere Konfiguration von Microsoft Excel 2013/2016/2019
- ✓ Sichere Konfiguration von Microsoft Office 2013/2016/2019
- ✓ Sichere Konfiguration von Microsoft Outlook 2013/2016/2019
- ✓ Sichere Konfiguration von Microsoft PowerPoint 2013/2016/2019
- ✓ Sichere Konfiguration von Microsoft Visio 2013/2016/2019

### Sicherheitsprinzipien

Bei vielen Anwendungsprodukten ist die Konfiguration häufig ein Kompromiss aus Sicherheit und Funktionalität. Je mehr die Sicherheit in den Fokus gerückt wird, desto mehr wird die Benutzerfunktionalität damit eingeschränkt. Administratoren stehen immer vor der Herausforderung, hier die Balance zu finden und sollten die Konfiguration der Produkte und der benötigten Funktionalität von dem benötigten Schutzbedarf der verarbeiteten Informationen abhängig machen.

Für die Bereitstellung einer sicheren Standardanwendungsfunktionalität ist es demnach nicht einfach, organisationsübergreifende Empfehlungen zur Verfügung zu stellen, die in unterschiedlichen Anwendungsszenarien zum Einsatz kommen, sowie unterschiedliche Schutzbedürfnisse haben. Die Empfehlungen wurden daher auf einer Reihe von Grundannahmen entwickelt, die im Folgenden kurz dargestellt werden:

- Für den Benutzer soll die Anzahl wichtiger Sicherheitsentscheidungen minimiert werden.
- Die benötigte Anwendungsfunktionalität soll nicht wesentlich beeinträchtigt werden.
- Nicht benötigte Funktionen sollen deaktiviert werden, um die Angriffsfläche zu verringern.
- Fokus auf Angriffsszenarien, die nach aktuellem Kenntnisstand auch ausgenutzt werden.
- Erhöhung des Datenschutzes, indem soweit wie möglich die Übertragungen von – für die Funktionalität nicht benötigte – Informationen an den Hersteller unterbunden wird.
- Erhöhung des Datenschutzes, indem externe Cloud-Dienste vermieden werden.

## Voraussetzungen

Die Sicherheit aller Microsoft Office-Produkte stützt sich auf die Sicherheit der Einsatzumgebung. Es wird daher vorausgesetzt, dass bereits

- entsprechende Richtlinien und bewährte Methoden zum Schutz der Organisationsinfrastruktur entwickelt wurden,
- aktuell branchenübliche Sicherheitstechniken eingesetzt werden sowie
- die im BSI-Grundschutz enthaltenen Empfehlungen und bewährten Methoden implementiert wurden.

## Gruppenrichtlinien

Im Folgenden werden die empfohlenen sicherheitsrelevanten Computerrichtlinien sowie Benutzerrichtlinien von Desktop- und Laptopcomputern aufgelistet. Diese können nur in Abhängigkeit von den Bedürfnissen innerhalb der Organisation umgesetzt werden. Wurde eine Active Directory-Umgebung innerhalb der gesamten Organisation bereitgestellt, auf denen die Office-Version ausgeführt wird, können diese über eine Gruppenrichtlinie zentral verwaltet werden. Da die Beschreibungen der jeweiligen Richtlinien im Editor für Gruppenrichtlinien zu finden sind, wird auf eine Darstellung im Dokument verzichtet.

Richtlinien sind von Microsoft standardmäßig auf „Nicht konfiguriert“ voreingestellt. Je nach Richtlinie kann das entweder einer aktivierten oder deaktivierten Einstellung entsprechen. In einigen wenigen Fällen hat eine nicht konfigurierte Einstellung eine eigene Bedeutung. Darüber hinaus kann „Nicht konfiguriert“ bedeuten, dass dem Nutzer die Einstellung im Office-Programm selbst überlassen wird.

Da es prinzipiell möglich ist, dass sich durch Updates die Bedeutung von „Nicht konfiguriert“ ändert, sollten alle Richtlinien durch den Administrator immer auf „Aktiviert“ () oder „Deaktiviert“ () und nur im Ausnahmefall auf „Nicht konfiguriert“ () gesetzt werden. Rot markierte Einstellungen kennzeichnen, dass die BSI-Empfehlungen von der durch Microsoft festgelegten Bedeutung von „Nicht konfiguriert“ abweichen. Sollte bei Aktivierung der Richtlinie eine Auswahl oder Eingabe notwendig sein, befindet sich diese im Falle einer konkreten Empfehlung in der Fußnote.

1.	<b>Onlineübersetzungs-Wörterbücher verwenden</b> <i>Use online translation dictionaries</i>	<input checked="" type="checkbox"/>
2.	<b>Alle nicht verwalteten Add-ins blockieren</b> <i>Block all unmanaged add-ins</i>	<input checked="" type="checkbox"/>
3.	<b>Liste der verwalteten Add-Ins</b> <i>List of managed add-ins</i>	<input checked="" type="checkbox"/>

<b>Elemente in Benutzeroberfläche deaktivieren\Benutzerdefiniert</b> <i>Disable Items in User Interface\Custom</i>		
4.	<b>Befehle deaktivieren</b> <i>Disable commands</i>	<input checked="" type="checkbox"/>
5.	<b>Tastenkombinationen deaktivieren</b> <i>Disable shortcut keys</i>	<input checked="" type="checkbox"/>

<b>Elemente in Benutzeroberfläche deaktivieren\Vordefiniert</b> <i>Disable Items in User Interface\Predefined</i>		
6.	<b>Befehle deaktivieren</b> <i>Disable commands</i>	<input checked="" type="checkbox"/>
7.	<b>Tastenkombinationen deaktivieren</b> <i>Disable shortcut keys</i>	<input checked="" type="checkbox"/>

<b>Word-Optionen\Erweitert</b> <i>Word Options\Advanced</i>		
8.	<b>Warnung zu benutzerdefiniertem Markup</b> <i>Custom markup warning</i>	<input checked="" type="checkbox"/> <sup>1</sup>
9.	<b>Automatische Verknüpfungen beim Öffnen aktualisieren</b> <i>Update automatic links at Open</i>	<input checked="" type="checkbox"/>

<b>Word-Optionen\Anzeigen</b> <i>Word Options\Display</i>		
10.	<b>Ausgeblendeten Text</b> <i>Hidden text</i>	<input checked="" type="checkbox"/>

<b>Word-Optionen\Sicherheit</b> <i>Word Options\Security</i>		
11.	<b>Ausgeblendete Markups anzeigen</b> <i>Make hidden markups visible</i>	<input checked="" type="checkbox"/>
12.	<b>Zufallszahl zur Verbesserung der Zusammenführungsgenauigkeit speichern</b> <i>Store random number to improve merge accuracy</i>	<input checked="" type="checkbox"/>
13.	<b>Dateiüberprüfung deaktivieren</b> <i>Turn off file validation</i>	<input checked="" type="checkbox"/>
14.	<b>Warnung anzeigen, bevor eine Datei, die Überarbeitungen oder Kommentare enthält, gedruckt, gespeichert oder versendet wird</b> <i>Warn before printing, saving or sending a file that contains tracked changes or comments</i>	<input checked="" type="checkbox"/>

15.	<b>Vor der Aktualisieren der Felder „IncludePicture“ und „IncludeText“ in Word keine Genehmigung anfordern</b> <i>Don't ask permission before updating IncludePicture and IncludeText fields in Word</i>	<input type="checkbox"/>
-----	---	--------------------------

<b>Word-Optionen\Sicherheit\Kryptografie</b> <i>Word Options\Security\Cryptography</i>		
16.	<b>Algorithmus für CNG-Zufallszahlen-Generator angeben</b> <i>Specify CNG random number generator algorithm</i>	<input checked="" type="checkbox"/> <sup>2</sup>
17.	<b>Anzahl für CNG-Kennwortwechsel festlegen</b> <i>Set CNG password spin count</i>	<input checked="" type="checkbox"/> <sup>3</sup>
18.	<b>Bei Kennwortänderung neuen Schlüssel verwenden</b> <i>Use new key on password change</i>	<input type="checkbox"/>
19.	<b>CNG-Chiffreverkettungsmodus konfigurieren</b> <i>Configure CNG cipher chaining mode</i>	<input checked="" type="checkbox"/> <sup>4</sup>
20.	<b>CNG-Chiffrieralgorithmus festlegen</b> <i>Set CNG cipher algorithm</i>	<input checked="" type="checkbox"/> <sup>5</sup>
21.	<b>CNG-Hashalgorithmus angeben</b> <i>Specify CNG hash algorithm</i>	<input checked="" type="checkbox"/> <sup>6</sup>
22.	<b>Länge des CNG-Chiffrierschlüssels festlegen</b> <i>Set CNG cipher key length</i>	<input checked="" type="checkbox"/> <sup>7</sup>
23.	<b>Länge für CNG-Salt angeben</b> <i>Specify CNG salt length</i>	<input checked="" type="checkbox"/> <sup>8</sup>
24.	<b>Parameter für CNG-Kontext festlegen</b> <i>Set parameters for CNG context</i>	<input type="checkbox"/>
25.	<b>Verschlüsselungskompatibilität angeben</b> <i>Specify encryption compatibility</i>	<input checked="" type="checkbox"/> <sup>9</sup>

<b>Word-Optionen\Sicherheit\Trust Center</b> <i>Word Options\Security\Trust Center</i>		
26.	<b>Alle Anwendungs-Add-Ins deaktivieren</b> <i>Disable all application add-ins</i>	<input type="checkbox"/>
27.	<b>Dynamischer Datenaustausch [nicht für Word 2013 verfügbar]</b> <i>Dynamic Data Exchange</i>	<input type="checkbox"/>
28.	<b>Ausführung von Makros in Office-Dateien aus dem Internet blockieren</b> <i>Block macros from running in Office files from the Internet</i>	<input checked="" type="checkbox"/>
29.	<b>Einstellungen für VBA-Makrobenachrichtigungen</b> <i>VBA Macro Notification Settings</i>	<input checked="" type="checkbox"/> <sup>10</sup>
30.	<b>Vertrauenswürdige Dokumente deaktivieren</b> <i>Turn off trusted documents</i>	<input type="checkbox"/>

2 RNG

3 100.000

4 CBC (Blockchiffreverkettung, Cipher Block Chaining)

5 AES

6 SHA512

7 256

8 16

9 Format der nächsten Generation verwenden

10 Alle Makros außer digital signierten Makros deaktivieren

31.	<b>Verschlüsselte Makros in Word Open XML-Dokumenten überprüfen</b> <i>Scan encrypted macros in Word Open XML documents</i>	<input checked="" type="checkbox"/> <sup>11</sup>
32.	<b>Anwendungs-Add-Ins müssen von einem vertrauenswürdigen Herausgeber signiert sein</b> <i>Require that application add-ins are signed by Trusted Publisher</i>	<input checked="" type="checkbox"/>
33.	<b>Vertrauenswürdige Dokumente im Netzwerk deaktivieren</b> <i>Turn off Trusted Documents on the network</i>	<input checked="" type="checkbox"/>
34.	<b>Zugriff auf Visual Basic-Project vertrauen</b> <i>Trust access to Visual Basic Project</i>	<input checked="" type="checkbox"/>
35.	<b>Benachrichtigungen für Vertrauensstellungsleiste für nicht signierte Anwendungs-Add-Ins deaktivieren und blockieren</b> <i>Disable Trust Bar Notification for unsigned application add-ins and block them</i>	<input checked="" type="checkbox"/>
36.	<b>Das Senden von eingebetteten TrueType-Schriftarten in Nachrichten zulassen [nicht für Word 2013 verfügbar]</b> <i>Allow embedded TrueType fonts to be sent in messages</i>	<input checked="" type="checkbox"/>

<b>Word-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz</b> <i>Word Options\Security\Trust Center\File Block Settings</i>		
37.	<b>Binärdokumente und Vorlagen im Format Word 2 und früher</b> <i>Word 2 and earlier binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>12</sup>
38.	<b>Binärdokumente und Vorlagen im Format Word 2007 und später</b> <i>Word 2007 and later binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>13</sup>
39.	<b>Dokumente und Vorlagen im Format Word 2007 und später</b> <i>Word 2007 and later documents and templates</i>	<input checked="" type="checkbox"/> <sup>14</sup>
40.	<b>Nur-Text-Dateien</b> <i>Plain text files</i>	<input checked="" type="checkbox"/> <sup>15</sup>
41.	<b>Office Open XML-Konverter für Word</b> <i>Office Open XML converters for Word</i>	<input checked="" type="checkbox"/> <sup>16</sup>
42.	<b>OpenDocument-Textdateien</b> <i>OpenDocument Text files</i>	<input checked="" type="checkbox"/> <sup>17</sup>
43.	<b>RTF-Dateien</b> <i>RTF files</i>	<input checked="" type="checkbox"/> <sup>18</sup>
44.	<b>Standardverhalten für Zugriffsschutz festlegen</b> <i>Set default file block behavior</i>	<input checked="" type="checkbox"/> <sup>19</sup>
45.	<b>Vorversionskonverter für Word</b> <i>Legacy converters for Word</i>	<input checked="" type="checkbox"/> <sup>20</sup>
46.	<b>Webseiten</b> <i>Web pages</i>	<input checked="" type="checkbox"/> <sup>21</sup>
47.	<b>Word 6.0-Binärdokumente und -vorlagen</b> <i>Word 6.0 binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>22</sup>

11 Verschlüsselte Makros überprüfen

12 Blockieren

13 Nicht blockieren

14 Nicht blockieren

15 Nicht blockieren

16 Nicht blockieren

17 Nicht blockieren

18 Nicht blockieren

19 Blockierte Dateien werden nicht geöffnet

20 Nicht blockieren

21 Nicht blockieren

22 Blockieren

48.	<b>Word 95-Binärdokumente und -vorlagen</b> <i>Word 95 binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>23</sup>
49.	<b>Word 97-Binärdokumente und -vorlagen</b> <i>Word 97 binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>24</sup>
50.	<b>Word 2000-Binärdokumente und -vorlagen</b> <i>Word 2000 binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>25</sup>
51.	<b>Word 2003-Binärdokumente und -vorlagen</b> <i>Word 2003 binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>26</sup>
52.	<b>Word 2003- und unformatierte XML-Dokumente</b> <i>Word 2003 and plain XML documents</i>	<input checked="" type="checkbox"/> <sup>27</sup>
53.	<b>Word XP-Binärdokumente und -vorlagen</b> <i>Word XP binary documents and templates</i>	<input checked="" type="checkbox"/> <sup>28</sup>

<b>Word-Optionen\Sicherheit\Trust Center\Geschützte Ansicht</b> <i>Word Options\Security\Trust Center\Protected View</i>		
54.	<b>Dateien an unsicheren Speicherorten nicht in der geschützten Ansicht öffnen</b> <i>Do not open files in unsafe locations in Protected View</i>	<input type="checkbox"/>
55.	<b>Dateien aus der Internetzone nicht in der geschützten Ansicht öffnen</b> <i>Do not open files from the Internet zone in Protected View</i>	<input type="checkbox"/>
56.	<b>Dateien mit lokalem UNC-Intranetpfad in geschützter Ansicht öffnen</b> <i>Open files on local Intranet UNC in Protected View</i>	<input type="checkbox"/>
57.	<b>Dokumentenverhalten bei Fehlschlagen der Dateiüberprüfung festlegen</b> <i>Set document behavior if file validation fails</i>	<input checked="" type="checkbox"/> <sup>29</sup>
58.	<b>Geschützte Ansicht für aus Outlook geöffnete Anlagen deaktivieren</b> <i>Turn off Protected View for attachments opened from Outlook</i>	<input type="checkbox"/>

<b>Word-Optionen\Sicherheit\Trust Center\Vertrauenswürdige Speicherorte</b> <i>Word Options\Security\Trust Center\Trusted Locations</i>		
59.	<b>Alle vertrauenswürdigen Speicherorte deaktivieren</b> <i>Disable all trusted locations</i>	<input checked="" type="checkbox"/>
60.	<b>Vertrauenswürdige Speicherorte im Netzwerk zulassen</b> <i>Allow Trusted Locations on the network</i>	<input type="checkbox"/>
61.	<b>Vertrauenswürdiger Speicherort #1 bis #20</b> <i>Trusted Location #1 to #20</i>	<input type="checkbox"/>

## Restrisiken

Die Konfiguration der Gruppenrichtlinien hilft nur dabei, die Angriffsfläche auf Anwendungen von Microsoft Word 2013/2016/2019 zu verringern bzw. die Sicherheit zu erhöhen. So existieren beispielsweise Verhaltensweisen, die nicht mittels Gruppenrichtlinien konfigurierbar sind. So können beispielsweise durch die Telemetrie auch sensible Daten an Microsoft übertragen werden.

23 Blockieren

24 Nicht blockieren

25 Nicht blockieren

26 Nicht blockieren

27 Nicht blockieren

28 Nicht blockieren

29 In geschützter Ansicht öffnen und Bearbeitung nicht zulassen

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an [info@cyber-allianz.de](mailto:info@cyber-allianz.de) gesendet werden.