



## EMPFEHLUNG: IT IN UNTERNEHMEN

# Sichere Konfiguration von Microsoft PowerPoint

## für den Einsatz auf dem Betriebssystem Microsoft Windows

Büroanwendungen gehören in vielen Organisationen zu den am häufigsten genutzten Anwendungsprogrammen. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen. Wegen ihrer großen Verbreitung und Angriffsfläche werden diese auch 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 PowerPoint 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. **Die Empfehlungen beziehen sich auf die Versionen 2016, 2019 und 2021 von Microsoft Word.** Bei Einsatz einer anderen Version lassen sich die Empfehlungen grundsätzlich für Entscheidungen zu einer Konfiguration unter Berücksichtigung möglicher Abweichungen ebenfalls heranziehen und anwenden.

Bei den vorliegenden Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft PowerPoint, die sicherheitsrelevant sind. Weitere Einstellungen finden sich in den BSI-Veröffentlichungen:

- ✓ Sichere Konfiguration von Microsoft Access
- ✓ Sichere Konfiguration von Microsoft Excel
- ✓ Sichere Konfiguration von Microsoft Office
- ✓ Sichere Konfiguration von Microsoft Outlook
- ✓ Sichere Konfiguration von Microsoft Visio
- ✓ Sichere Konfiguration von Microsoft Word

### 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 Ba-

lance 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 anhand 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 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.

<b>Verschiedenes</b> <i>Miscellaneous</i>		
1.	<b>Folienaktualisierung deaktivieren</b> <i>Disable Slide Update</i>	<input checked="" type="checkbox"/>
2.	<b>Liste der verwalteten Add-Ins</b> <i>List of managed add-ins</i>	<input checked="" type="checkbox"/>
3.	<b>Alle nicht verwalteten Add-Ins blockieren</b> <i>Block all unmanaged 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>PowerPoint-Optionen\Sicherheit</b> <i>PowerPoint Options\Security</i>		
8.	<b>Ausgeblendete Markups anzeigen</b> <i>Make hidden markups visible</i>	<input checked="" type="checkbox"/>
9.	<b>Verschlüsselte Makros in PowerPoint Open XML-Präsentationen überprüfen</b> <i>Scan encrypted macros in PowerPoint Open XML presentations</i>	<input checked="" type="checkbox"/> <sup>1</sup>
10.	<b>Programme ausführen</b> <i>Run Programs</i>	<input checked="" type="checkbox"/> <sup>2</sup>
11.	<b>Dateiüberprüfung deaktivieren</b> <i>Turn off file validation</i>	<input checked="" type="checkbox"/>
12.	<b>Blockierung des automatischen Downloads von verknüpften Bildern aufheben</b> <i>Unblock automatic download of linked images</i>	<input checked="" type="checkbox"/>

<b>PowerPoint-Optionen\Sicherheit\Kryptografie</b> <i>PowerPoint Options\Security\Cryptography</i>		
13.	<b>Länge für CNG-Salt angeben</b> <i>Specify CNG salt length</i>	<input checked="" type="checkbox"/> <sup>3</sup>
14.	<b>Anzahl für CNG-Kennwortwechsel festlegen</b> <i>Set CNG password spin count</i>	<input checked="" type="checkbox"/> <sup>4</sup>

1 Verschlüsselte Makros überprüfen

2 Deaktivieren (keine Programme ausführen)

3 16

4 100.000

15.	<b>CNG-Hashalgorithmus angeben</b> <i>Specify CNG hash algorithm</i>	<input checked="" type="checkbox"/> <sup>5</sup>
16.	<b>Länge des CNG-Chiffrierschlüssels festlegen</b> <i>Set CNG cipher key length</i>	<input checked="" type="checkbox"/> <sup>6</sup>
17.	<b>CNG-Chiffrieralgorithmus festlegen</b> <i>Set CNG cipher algorithm</i>	<input checked="" type="checkbox"/> <sup>7</sup>
18.	<b>Verschlüsselungskompatibilität angeben</b> <i>Specify encryption compatibility</i>	<input checked="" type="checkbox"/> <sup>8</sup>
19.	<b>Algorithmus für CNG-Zufallszahlen-Generator angeben</b> <i>Specify CNG random number generator algorithm</i>	<input checked="" type="checkbox"/> <sup>9</sup>
20.	<b>Bei Kennwortänderung neuen Schlüssel verwenden</b> <i>Use new key on password change</i>	<input type="checkbox"/>
21.	<b>Parameter für CNG-Kontext festlegen</b> <i>Set parameters for CNG context</i>	<input type="checkbox"/>
22.	<b>CNG-Chiffreverkettungsmodus konfigurieren</b> <i>Configure CNG cipher chaining mode</i>	<input checked="" type="checkbox"/> <sup>10</sup>

<b>PowerPoint-Optionen\Sicherheit\Trust Center</b> <i>PowerPoint Options\Security\Trust Center</i>		
23.	<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"/>
24.	<b>Zugriff auf Visual Basic-Project vertrauen</b> <i>Trust access to Visual Basic Project</i>	<input type="checkbox"/>
25.	<b>Vertrauenswürdige Dokumente im Netzwerk deaktivieren</b> <i>Turn off Trusted Documents on the network</i>	<input type="checkbox"/>
26.	<b>Alle Anwendungs-Add-Ins deaktivieren</b> <i>Disable all application add-ins</i>	<input type="checkbox"/>
27.	<b>Vertrauenswürdige Dokumente deaktivieren</b> <i>Turn off trusted documents</i>	<input type="checkbox"/>
28.	<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"/>
29.	<b>Einstellungen für VBA-Makrobenachrichtigungen</b> <i>VBA Macro Notification Settings</i>	<input checked="" type="checkbox"/> <sup>11</sup>
30.	<b>Blockieren der Ausführung von Makros in Office-Dateien aus dem Internet</b> <i>Block macros from running in Office files from the Internet</i>	<input checked="" type="checkbox"/>
31.	<b>Maximale Anzahl beizubehaltender Vertrauensstellungs-Datensätze festlegen</b> <i>Set maximum number of trust records to preserve</i>	<input checked="" type="checkbox"/> <sup>12</sup>
32.	<b>Maximale Anzahl vertrauenswürdiger Dokumente festlegen</b> <i>Set maximum number of trusted documents</i>	<input checked="" type="checkbox"/> <sup>13</sup>

5 SHA512

6 256

7 AES

8 Format der nächsten Generation verwenden

9 RNG

10 CBC (Blockchiffreverkettung, Cipher Block Chaining)

11 Alle Makros außer digital signierten Makros deaktivieren

12 400

13 500

PowerPoint-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz <i>PowerPoint Options\Security\Trust Center\File Block Settings</i>		
33.	<b>Standardverhalten für Zugriffsschutz festlegen</b> <i>Set default file block behavior</i>	<input checked="" type="checkbox"/> <sup>14</sup>
34.	<b>PowerPoint-Betakonverter</b> <i>PowerPoint beta converters</i>	<input checked="" type="checkbox"/> <sup>15</sup>
35.	<b>Gliederungsdateien</b> <i>Outline files</i>	<input checked="" type="checkbox"/> <sup>16</sup>
36.	<b>PowerPoint-Betadateien</b> <i>PowerPoint beta files</i>	<input checked="" type="checkbox"/> <sup>17</sup>
37.	<b>Webseiten</b> <i>Web pages</i>	<input checked="" type="checkbox"/> <sup>18</sup>
38.	<b>Präsentationen, Bildschirmpräsentationen, Vorlagen, Designs und Add-In-Dateien im Format PowerPoint 2007 und später</b> <i>PowerPoint 2007 and later presentations, shows, templates, themes and add-in files</i>	<input checked="" type="checkbox"/> <sup>19</sup>
39.	<b>Microsoft Office Open XML-Konverter für PowerPoint</b> <i>Microsoft Office Open XML converters for PowerPoint</i>	<input checked="" type="checkbox"/> <sup>20</sup>
40.	<b>OpenDocument-Präsentationsdateien</b> <i>OpenDocument Presentation files</i>	<input checked="" type="checkbox"/> <sup>21</sup>
41.	<b>Vorversionskonverter für PowerPoint</b> <i>Legacy converters for PowerPoint</i>	<input checked="" type="checkbox"/> <sup>22</sup>
42.	<b>PowerPoint 97-2003-Präsentationen, -Bildschirmpräsentationen, -Vorlagen und -Add-In-Dateien</b> <i>PowerPoint 97-2003 presentations, shows, templates and add-in files</i>	<input checked="" type="checkbox"/> <sup>23</sup>
43.	<b>Grafikfilter</b> <i>Graphic Filters</i>	<input checked="" type="checkbox"/> <sup>24</sup>

PowerPoint-Optionen\Sicherheit\Trust Center\Geschützte Ansicht <i>PowerPoint Options\Security\Trust Center\Protected View</i>		
44.	<b>Dokumentenverhalten bei Fehlschlagen der Dateiüberprüfung festlegen</b> <i>Set document behavior if file validation fails</i>	<input checked="" type="checkbox"/> <sup>25</sup>
45.	<b>Keine Dateien aus der Internetzone in der geschützten Ansicht öffnen</b> <i>Do not open files from the Internet zone in Protected View</i>	<input type="checkbox"/>
46.	<b>Geschützte Ansicht für aus Outlook geöffnete Anlagen deaktivieren</b> <i>Turn off Protected View for attachments opened from Outlook</i>	<input type="checkbox"/>
47.	<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"/>
48.	<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"/>

14 Blockierte Dateien werden nicht geöffnet

15 Nicht blockieren

16 Nicht blockieren

17 Nicht blockieren

18 Nicht blockieren

19 Nicht blockieren

20 Nicht blockieren

21 Nicht blockieren

22 Nicht blockieren

23 Nicht blockieren

24 Nicht blockieren

25 In geschützter Ansicht öffnen und Bearbeitung nicht zulassen

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

## Restrisiken

Die Konfiguration der Gruppenrichtlinien hilft nur dabei, die Angriffsfläche auf Anwendungen von Microsoft PowerPoint 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.

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.