



## EMPFEHLUNG: IT IN UNTERNEHMEN

# Sichere Konfiguration von Microsoft Office

## 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 Office 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 Office.** 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 Computer- und Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft Office, 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 Outlook
- ✓ Sichere Konfiguration von Microsoft PowerPoint
- ✓ 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 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 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 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.

## Computerrichtlinien

### Aktualisierungen

Updates

1.	<b>Automatische Updates aktivieren</b> <i>Enable Automatic Updates</i>	<input checked="" type="checkbox"/>
2.	<b>Aktualisierungspfad</b> <i>Update Path</i>	<input checked="" type="checkbox"/> <sup>1</sup>
3.	<b>Option zum Aktivieren oder Deaktivieren von Updates ausblenden</b> <i>Hide option to enable or disable updates</i>	<input checked="" type="checkbox"/>
4.	<b>Upgrade von Office 2019 auf Microsoft 365 Apps for Enterprise</b> <i>Upgrade Office 2019 to Microsoft 365 Apps for enterprise</i>	<input checked="" type="checkbox"/>

<b>Sicherheitseinstellungen</b> <i>Security Settings</i>		
5.	<b>Grafikfilterimport</b> <i>Graphics filter import</i>	<input checked="" type="checkbox"/>
6.	<b>Kennwortzwischenlagerung deaktivieren</b> <i>Disable Password Caching</i>	<input checked="" type="checkbox"/>
7.	<b>VBA für Office-Anwendungen deaktivieren</b> <i>Disable VBA for Office applications</i>	<input checked="" type="checkbox"/>
8.	<b>Paketreparatur deaktivieren</b> <i>Disable Package Repair</i>	<input checked="" type="checkbox"/>

<b>Sicherheitseinstellungen\IE-Sicherheit</b> <i>Security Settings\IE Security</i>		
9.	<b>ActiveX-Installation einschränken</b> <i>Restrict ActiveX Install</i>	<input checked="" type="checkbox"/>
10.	<b>Dateidownload einschränken</b> <i>Restrict File Download</i>	<input checked="" type="checkbox"/>
11.	<b>Add-On-Verwaltung</b> <i>Add-on Management</i>	<input checked="" type="checkbox"/>
12.	<b>Sperrung der Zone des lokalen Computers</b> <i>Local Machine Zone Lockdown Security</i>	<input checked="" type="checkbox"/>
13.	<b>Konsistente MIME-Verarbeitung</b> <i>Consistent Mime Handling</i>	<input checked="" type="checkbox"/>
14.	<b>Sicherheitsfeature für MIME-Ermittlung</b> <i>Mime Sniffing Safety Feature</i>	<input checked="" type="checkbox"/>
15.	<b>Objektzwischenlagerungsschutz</b> <i>Object Caching Protection</i>	<input checked="" type="checkbox"/>
16.	<b>Sicherheitseinschränkungen für Skriptfenster</b> <i>Scripted Window Security Restrictions</i>	<input checked="" type="checkbox"/>
17.	<b>Schutz vor Zonenanhebung</b> <i>Protection from Zone Elevation</i>	<input checked="" type="checkbox"/>
18.	<b>Informationsleiste</b> <i>Information Bar</i>	<input checked="" type="checkbox"/>
19.	<b>Benutzername und Kennwort deaktivieren</b> <i>Disable user name and password</i>	<input checked="" type="checkbox"/>
20.	<b>Binden an Objekt</b> <i>Bind to object</i>	<input checked="" type="checkbox"/>

1 Pfad zum Speicherort

21.	<b>Gespeichert von URL</b> <i>Saved from URL</i>	<input checked="" type="checkbox"/>
22.	<b>URL navigieren</b> <i>Navigate URL</i>	<input checked="" type="checkbox"/>
23.	<b>Popups blockieren</b> <i>Block popups</i>	<input checked="" type="checkbox"/>

## Benutzerrichtlinien

<b>Dokumentinformationsbereich</b> <i>Document Information Panel</i>		
24.	<b>Dokumenteninformationsbereich für Signal übertragende Elemente der Benutzeroberfläche</b> <i>Document Information Panel Beaconsing UI</i>	<input checked="" type="checkbox"/> <sup>2</sup>
25.	<b>Dokumenteninformationsbereich deaktivieren</b> <i>Disable Document Information Panel</i>	<input checked="" type="checkbox"/>

<b>Add-Ins Microsoft „Speichern als PDF“ und „Speichern als XPS“</b> <i>Microsoft Save As PDF and XPS add-ins</i>		
26.	<b>Einschließen von Dokumenteigenschaften in PDF- und XPS-Ausgabe deaktivieren</b> <i>Disable inclusion of document properties in PDF and XPS output</i>	<input checked="" type="checkbox"/>

<b>Eingeschränkte Berechtigungen verwalten</b> <i>Manage Restricted Permissions</i>		
27.	<b>Benutzer können Berechtigungen für Inhalte, deren Rechte verwaltet werden, nicht ändern</b> <i>Prevent users from changing permissions on rights managed content</i>	<input checked="" type="checkbox"/>
28.	<b>Benutzer mit früheren Versionen von Office können mit Browsern lesen...</b> <i>Allow users with earlier versions of Office to read with browsers...</i>	<input checked="" type="checkbox"/>
29.	<b>Benutzer müssen zum Überprüfen der Berechtigung immer eine Verbindung herstellen</b> <i>Always require users to connect to verify permission</i>	<input checked="" type="checkbox"/>
30.	<b>Gruppen in Office immer erweitern, wenn die Berechtigung für Dokumente eingeschränkt wird</b> <i>Always expand groups in Office when restricting permission for documents</i>	<input checked="" type="checkbox"/>
31.	<b>Benutzer können nie Gruppen angeben, wenn die Berechtigung für Dokumente eingeschränkt wird</b> <i>Never allow users to specify groups when restricting permission for documents</i>	<input checked="" type="checkbox"/>
32.	<b>Berechtigungsrichtlinien-Standardserver für Symbolleiste für den Schnellzugriff angeben</b> <i>Specify Permission Policy Default Server for Quick Access Toolbar</i>	<input checked="" type="checkbox"/> <sup>3</sup>

<b>Telemetriedashboard</b> <i>Telemetry Dashboard</i>		
33.	<b>Telemetrie-Datensammlung aktivieren</b> <i>Turn on telemetry data collection</i>	<input checked="" type="checkbox"/>
34.	<b>Datenschutzinstellungen im Office-Telemetrie-Agent aktivieren</b> <i>Turn on privacy settings in Office Telemetry Agent</i>	<input checked="" type="checkbox"/>

<sup>2</sup> Benutzeroberfläche immer anzeigen

<sup>3</sup> Lokale IP-Adresse, z.B. 127.0.0.1

35.	<b>Hochladen von Daten für den Office-Telemetrie-Agent</b> <i>Turn on data uploading for Office Telemetry Agent</i>	<input checked="" type="checkbox"/>
-----	--	-------------------------------------

**Smart Document's (Word, Excel)***Smart Documents (Word, Excel)*

36.	<b>Manifestverwendung durch Smart Document's deaktivieren</b> <i>Disable Smart Document's use of manifests</i>	<input checked="" type="checkbox"/>
-----	---	-------------------------------------

**Signieren***Signing*

37.	<b>Office-Signaturanbieter unterdrücken</b> <i>Suppress Office Signing Providers</i>	<input checked="" type="checkbox"/> <sup>4</sup>
38.	<b>Menüelement für externe Signaturdienste unterdrücken</b> <i>Suppress external signatures services menu item</i>	<input checked="" type="checkbox"/>
39.	<b>Vorversions-Formatsignaturen</b> <i>Legacy format signatures</i>	<input checked="" type="checkbox"/>
40.	<b>EKU-Filterung</b> <i>EKU filtering</i>	<input checked="" type="checkbox"/>

**Servereinstellungen***Server Settings*

41.	<b>Abrufen veröffentlichter Hyperlinks von SharePoint Server durch den Office-Client deaktivieren</b> <i>Disable the Office client from polling the SharePoint Server for published links</i>	<input checked="" type="checkbox"/>
-----	--	-------------------------------------

**Verschiedenes***Miscellaneous*

42.	<b>OneDrive-Anmeldung anzeigen</b> <i>Show OneDrive Sign In</i>	<input checked="" type="checkbox"/>
43.	<b>Screenshots nicht automatisch mit einem Link versehen</b> <i>Do not automatically hyperlink screenshots</i>	<input checked="" type="checkbox"/>
44.	<b>Anmeldung bei Office blockieren</b> <i>Block signing into Office</i>	<input checked="" type="checkbox"/> <sup>5</sup>
45.	<b>Steuerelementbloggen</b> <i>Control Blogging</i>	<input checked="" type="checkbox"/> <sup>6</sup>

**Globale Optionen\Benutzerdefiniert***Global Options\Customize*

46.	<b>Alle Benutzeranpassungen deaktivieren</b> <i>Turn off all user customizations</i>	<input checked="" type="checkbox"/>
47.	<b>Benutzeroberflächenerweiterung von Dokumenten und Vorlagen deaktivieren</b> <i>Disable UI extending from documents and templates</i>	<input checked="" type="checkbox"/>

4 Westlich und Ostasiatisch aktivieren

5 Keine zulässig

6 Deaktiviert

<b>Online präsentieren</b> <i>Present Online</i>		
48.	<b>Office-Präsentationsdienst aus der Liste der Onlinepräsentationsdienste in PowerPoint und Word entfernen</b> <i>Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word</i>	<input checked="" type="checkbox"/>
49.	<b>Einschränken des programmgesteuerten Zugriffs für das Erstellen von Onlinepräsentationen in PowerPoint und Word</b> <i>Restrict programmatic access for creating online presentations in PowerPoint and Word</i>	<input checked="" type="checkbox"/>
50.	<b>Verhindern, dass Benutzer Onlinepräsentationsdienste in PowerPoint und Word hinzufügen können</b> <i>Prevent users from adding online presentation services in PowerPoint and Word</i>	<input checked="" type="checkbox"/>

<b>Online präsentieren\Präsentationsdienste</b> <i>Present Online\Presentation Services</i>		
51.	<b>Präsentationsdienst in PowerPoint und Word konfigurieren #1 bis #10</b> <i>Configure presentation service in PowerPoint and Word #1 to #10</i>	<input checked="" type="checkbox"/>

<b>Datenschutz\Trust Center</b> <i>Privacy\Trust Center</i>		
52.	<b>Bestätigungs-Assistenten bei der ersten Ausführung deaktivieren</b> <i>Disable Opt-in Wizard on first run</i>	<input checked="" type="checkbox"/>
53.	<b>Automatisches Empfangen kleiner Updates zur Verbesserung der Zuverlässigkeit</b> <i>Automatically receive small updates to improve reliability</i>	<input checked="" type="checkbox"/>
54.	<b>Programm zur Verbesserung der Benutzerfreundlichkeit aktivieren</b> <i>Enable Customer Experience Improvement Program</i>	<input checked="" type="checkbox"/>
55.	<b>Die Verwendung verbundener Erfahrungen in Office zulassen</b> <i>Allow the use of connected experiences in Office</i>	<input checked="" type="checkbox"/>
56.	<b>Die Verwendung verbundener Erfahrungen, die Inhalt analysieren, in Office zulassen</b> <i>Allow the use of connected experiences in Office that analyze content</i>	<input checked="" type="checkbox"/>
57.	<b>Die Verwendung verbundener Erfahrungen, die Onlineinhalte herunterladen, in Office zulassen</b> <i>Allow the use of connected experiences in Office that download online content</i>	<input checked="" type="checkbox"/>
58.	<b>Die Verwendung zusätzlicher optionaler verbundener Erfahrungen in Office zulassen</b> <i>Allow the use of additional optional connected experiences in Office</i>	<input checked="" type="checkbox"/>
59.	<b>Stufe der von Office an Microsoft gesendeten Clientsoftware-Diagnosedaten konfigurieren</b> <i>Configure the level of client software diagnostic data sent by Office to Microsoft</i>	<input checked="" type="checkbox"/> <sup>7</sup>
60.	<b>Persönliche Informationen senden</b> <i>Send personal information</i>	<input checked="" type="checkbox"/>

<b>Dienste</b> <i>Services</i>		
61.	<b>Office-Roamingbenutzereinstellungen deaktivieren</b> <i>Disable Roaming Office User Settings</i>	<input checked="" type="checkbox"/>

7 Weder noch

Dienste\Fax Services\Fax		
62.	<b>Internetfaxfeature deaktivieren</b> <i>Disable Internet Fax feature</i>	<input checked="" type="checkbox"/>

Extras Optionen Allgemein Dienstoptionen\Onlineinhalte Tools   Options   General   Service Options...\Online Content		
63.	<b>Onlineinhalteoptionen</b> <i>Online Content Options</i>	<input checked="" type="checkbox"/> <sup>8</sup>

Extras Optionen Allgemein Weboptionen\Dateien Tools   Options   General   Web Options...\Files		
64.	<b>Office-Dokumente beim Browsen mit Lese-/Schreibzugriff senden</b> <i>Open Office documents as read/write while browsing</i>	<input type="checkbox"/>

Extras Optionen Rechtschreibung\Rechtschreibprüfung für Datensammlung Tools   Options   Spelling\Proofing Data Collection		
65.	<b>Korrekturhilfen verbessern</b> <i>Improve Proofing Tools</i>	<input type="checkbox"/>

Sicherheitseinstellungen Security Settings		
66.	<b>Benutzeroberfläche für PDF-Verschlüsselungseinstellung deaktivieren</b> <i>Turn off PDF encryption setting UI</i>	<input type="checkbox"/>
67.	<b>OLE-Objekte überprüfen</b> <i>Check OLE objects</i>	<input checked="" type="checkbox"/> <sup>9</sup>
68.	<b>Excel-RTD-Server überprüfen</b> <i>Check Excel RTD servers</i>	<input type="checkbox"/>
69.	<b>Verschlüsselungstyp für kennwortgeschützte Office Open XML-Dateien</b> <i>Encryption type for password protected Office Open XML files</i>	<input checked="" type="checkbox"/> <sup>10</sup>
70.	<b>Mindestlänge für Kennwort festlegen</b> <i>Set minimum password length</i>	<input checked="" type="checkbox"/>
71.	<b>Automatisierungssicherheit</b> <i>Automation Security</i>	<input checked="" type="checkbox"/> <sup>11</sup>
72.	<b>Alle ActiveX-Steuerelemente deaktivieren</b> <i>Disable all ActiveX</i>	<input checked="" type="checkbox"/>
73.	<b>Kennwort zum Öffnen der Benutzeroberfläche deaktivieren</b> <i>Disable password to open UI</i>	<input type="checkbox"/>
74.	<b>Dokumentmetadaten für kennwortgeschützte Dateien schützen</b> <i>Protect document metadata for password protected files</i>	<input checked="" type="checkbox"/>
75.	<b>OWC-Datenquellenanbieter überprüfen</b> <i>Check OWC data source providers</i>	<input checked="" type="checkbox"/>

8 Für Office keine Internetverbindungen zulassen

9 IE-Killbitliste außer Kraft setzen

10 Microsoft Enhanced RSA und AES Cryptographic Provider, AES-256, 256-Bit

11 Makros standardmäßig deaktivieren

76.	<b>Verschlüsselungstyp für kennwortgeschützte Office 97-2003-Dateien</b> <i>Encryption type for password protected Office 97-2003 files</i>	<input checked="" type="checkbox"/> <sup>12</sup>
77.	<b>Linkwarnungen unterdrücken</b> <i>Suppress hyperlink warnings</i>	<input checked="" type="checkbox"/>
78.	<b>ActiveX-Objekte überprüfen</b> <i>Check ActiveX objects</i>	<input checked="" type="checkbox"/> <sup>13</sup>
79.	<b>Fehlerberichterstattung für Dateien mit Dateiüberprüfungsfehlern deaktivieren</b> <i>Turn off error reporting for files that fail file validation</i>	<input checked="" type="checkbox"/>
80.	<b>Dokumenteigenschaften verschlüsseln</b> <i>Encrypt document properties</i>	<input checked="" type="checkbox"/>
81.	<b>Dokumentmetadaten für Office Open XML-Dateien, deren Rechte verwaltet werden, schützen</b> <i>Protect document metadata for rights managed Office Open XML Files</i>	<input checked="" type="checkbox"/>
82.	<b>VBA für Office-Anwendungen deaktivieren</b> <i>Disable VBA for Office applications</i>	<input checked="" type="checkbox"/>
83.	<b>Steuerelemente in Forms3 laden</b> <i>Load Controls in Forms3</i>	<input checked="" type="checkbox"/> <sup>14</sup>
84.	<b>In Word und Excel können keine verwalteten Codeerweiterungen geladen werden</b> <i>Prevent Word and Excel from loading managed code extensions</i>	<input checked="" type="checkbox"/>
85.	<b>Regelstufe für Kennwort festlegen</b> <i>Set password rules level</i>	<input checked="" type="checkbox"/> <sup>15</sup>
86.	<b>ActiveX-Steuerelementinitialisierung</b> <i>ActiveX Control Initialization</i>	<input checked="" type="checkbox"/> <sup>16</sup>
87.	<b>Kennworthashformat als ISO-kompatibel festlegen</b> <i>Set password hash format as ISO-compliant</i>	<input checked="" type="checkbox"/>
88.	<b>Domänentimeout für Kennwortregeln festlegen</b> <i>Set password rules domain timeout</i>	<input checked="" type="checkbox"/> <sup>17</sup>
89.	<b>Alle Benachrichtigungen für Vertrauensstellungsleiste aus Sicherheitsgründen deaktivieren</b> <i>Disable all Trust Bar notifications for security issues</i>	<input checked="" type="checkbox"/>
90.	<b>Zulassen, dass VBA Typbibliotheksverweise über Pfade von nicht vertrauenswürdigen Intranet-Speicherorten lädt</b> <i>Allow VBA to load typelib references by path from untrusted intranet locations</i>	<input checked="" type="checkbox"/>
91.	<b>Zusätzliche Sicherheitsüberprüfungen von VBA-Bibliotheksverweisen deaktivieren, die möglicherweise auf unsichere Speicherorte auf dem lokalen Computer verweisen</b> <i>Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine</i>	<input checked="" type="checkbox"/>
92.	<b>Anpassungen von VSTO 2003 und 2005 auf Dokumentenebene deaktivieren</b> <i>Disable VSTO 2003 and 2005 document-level customizations</i>	<input checked="" type="checkbox"/>
93.	<b>Minimierung des Ungültigmachens von digitalen VBA-Projekt Signaturen aktivieren</b> <i>Enable Minimizing VBA Project Digital Signature Invalidation</i>	<input checked="" type="checkbox"/>

**Sicherheitseinstellungen\Digitale Signaturen**

Security Settings\Digital Signatures

12 Microsoft Enhanced RSA und AES Cryptographic Provider, AES-256, 256-Bit

13 IE-Killbitliste außer Kraft setzen

14 1

15 Prüfung der lokalen Länge und lokalen Komplexität und Domänenrichtlinienprüfungen

16 4

17 4.000



94.	<b>OCSP zum Signaturgenerierungs-Zeitpunkt anfordern</b> <i>Require OCSP at signature generation time</i>	<input checked="" type="checkbox"/>
95.	<b>XadES-Mindeststufe für digitale Signaturgenerierung angeben</b> <i>Specify minimum XadES level for digital signature generation</i>	<input checked="" type="checkbox"/> <sup>18</sup>
96.	<b>XadES-Teile einer digitalen Signatur überprüfen</b> <i>Check the XadES portions of a digital signature</i>	<input checked="" type="checkbox"/>
97.	<b>Beim Überprüfen von Signaturen keine abgelaufenen Zertifikate zulassen</b> <i>Do not allow expired certificates when validating signatures</i>	<input checked="" type="checkbox"/>
98.	<b>Hashalgorithmus für digitale Signatur auswählen</b> <i>Select digital signature hashing algorithm</i>	<input checked="" type="checkbox"/> <sup>19</sup>
99.	<b>Zeitstempel-Hashalgorithmus konfigurieren</b> <i>Configure time stamping hashing algorithm</i>	<input checked="" type="checkbox"/> <sup>20</sup>
100.	<b>Vorversions-Hashalgorithmus konfigurieren</b> <i>Configure legacy hashing algorithm</i>	<input checked="" type="checkbox"/> <sup>21</sup>
101.	<b>Ungültigen Hashalgorithmus konfigurieren</b> <i>Configure invalid hashing algorithm</i>	<input checked="" type="checkbox"/> <sup>22</sup>
102.	<b>Mindestgröße für öffentlichen RSA-Schlüssel konfigurieren</b> <i>Configure minimum RSA public key size</i>	<input checked="" type="checkbox"/> <sup>23</sup>
103.	<b>Größe für öffentlichen RSA-Vorversionsschlüssel konfigurieren</b> <i>Configure legacy RSA public key size</i>	<input checked="" type="checkbox"/> <sup>24</sup>
104.	<b>Größe für ungültigen öffentlichen RSA-Schlüssel konfigurieren</b> <i>Configure invalid RSA public key size</i>	<input checked="" type="checkbox"/> <sup>25</sup>
105.	<b>Mindestgröße für öffentlichen DSA-Schlüssel konfigurieren</b> <i>Configure minimum DSA public key size</i>	<input checked="" type="checkbox"/> <sup>26</sup>
106.	<b>Größe für öffentlichen DSA-Vorversionsschlüssel konfigurieren</b> <i>Configure legacy DSA public key size</i>	<input checked="" type="checkbox"/> <sup>27</sup>
107.	<b>Größe für ungültigen öffentlichen DSA-Schlüssel konfigurieren</b> <i>Configure invalid DSA public key size</i>	<input checked="" type="checkbox"/> <sup>28</sup>
108.	<b>Zertifikatausstellerfilter angeben</b> <i>Specify filtering for certificate issuers</i>	<input checked="" type="checkbox"/>
109.	<b>Namen des Zeitstempelservers angeben</b> <i>Specify timestamp server name</i>	<input checked="" type="checkbox"/>
110.	<b>Timeout für Zeitstempelserver angeben</b> <i>Set timestamp server timeout</i>	<input checked="" type="checkbox"/> <sup>29</sup>
111.	<b>Signaturüberprüfungsstufe festlegen</b> <i>Set signature verification level</i>	<input checked="" type="checkbox"/> <sup>30</sup>
112.	<b>Erforderliche XadES-Stufe für Signaturgenerierung</b> <i>Requested XadES level for signature generation</i>	<input checked="" type="checkbox"/> <sup>31</sup>

18 Keine Mindeststufe

19 SHA512

20 SHA512

21 SHA1

22 SHA1

23 1024

24 512

25 512

26 1024

27 1024

28 512

29 5

30 Office 2013-Regeln

31 XadES-X-L

113.	<b>Alternative Zertifikatsanbieter anzeigen</b> <i>Display alternative certificate providers</i>	<input type="checkbox"/>
------	---	--------------------------

<b>Sicherheitseinstellungen\Hinterlegte Zertifikate</b> <i>Security Settings\Escrow Certificates</i>		
114.	<b>Hinterlegter Schlüssel #1 bis #20</b> <i>Escrow Key #1 to #20</i>	<input type="checkbox"/>

<b>Sicherheitseinstellungen\Trust Center</b> <i>Security Settings\Trust Center</i>		
115.	<b>Vertrauenswürdiger Speicherort #1 bis #20</b> <i>Trusted Locations #1 to #20</i>	<input type="checkbox"/>
116.	<b>Mischung aus Richtlinien- und Benutzerspeicherorten zulassen</b> <i>Allow mix of policy and user locations</i>	<input type="checkbox"/>
117.	<b>Das mindestens erforderliche Betriebssystem für die Überprüfung von agilen VBA-Signaturen festlegen</b> <i>Set the minimum operating system for verifying agile VBA signatures</i>	<input checked="" type="checkbox"/> <sup>32</sup>
118.	<b>Nur VBA-Makros vertrauen, die V3-Signaturen verwenden</b> <i>Only trust VBA macros that use V3 signatures</i>	<input checked="" type="checkbox"/>

<b>Sicherheitseinstellungen\Trust Center\Geschützte Ansicht</b> <i>Security Settings\Trust Center\Protected View</i>		
119.	<b>Unsicherer Speicherort #1 bis #20</b> <i>Unsafe Location #1 to #20</i>	<input type="checkbox"/>

<b>Sicherheitseinstellungen\Trust Center\Vertrauenswürdige Kataloge</b> <i>Security Settings\Trust Center\Trusted Catalogs</i>		
120.	<b>Vertrauenswürdiger Katalog-Speicherort #1 bis #10</b> <i>Trusted Catalog Location #1 to #10</i>	<input type="checkbox"/>
121.	<b>Unsichere Web-Add-Ins und Kataloge zulassen</b> <i>Allow Unsecure web add-ins and Catalogs</i>	<input type="checkbox"/>
122.	<b>Web-Add-Ins blockieren</b> <i>Block Web-Add-ins</i>	<input checked="" type="checkbox"/>
123.	<b>Office Store blockieren</b> <i>Block the Office Store</i>	<input checked="" type="checkbox"/>

## Restrisiken

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