Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN UNTERNEHMEN

Sichere Konfiguration von Microsoft Word

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 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 Word , 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 PowerPoint
- ✔ Sichere Konfiguration von Microsoft Visio

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.

Verschiedenes *Miscellaneous*		
1.	**Onlineübersetzungs-Wörterbücher verwenden** *Use online translation dictionaries*	☑
2.	**Alle nicht verwalteten Add-ins blockieren** *Block all unmanaged add-ins*	☑
3.	**Liste der verwalteten Add-Ins** *List of managed add-ins*	☑

Elemente in Benutzeroberfläche deaktivieren\Benutzerdefiniert *Disable Items in User Interface\Custom*		
4.	**Befehle deaktivieren** *Disable commands*	☒
5.	**Tastenkombinationen deaktivieren** *Disable shortcut keys*	☒

Elemente in Benutzeroberfläche deaktivieren\Vordefiniert *Disable Items in User Interface\Predefined*		
6.	**Befehle deaktivieren** *Disable commands*	☒
7.	**Tastenkombinationen deaktivieren** *Disable shortcut keys*	☒

Word-Optionen\Erweitert *Word Options\Advanced*		
8.	**Warnung zu benutzerdefiniertem Markup** *Custom markup warning*	☑[1]
9.	**Automatische Verknüpfungen beim Öffnen aktualisieren** *Update automatic links at Open*	☒

Word-Optionen\Anzeigen *Word Options\Display*		
10.	**Ausgeblendeten Text** *Hidden text*	☑

Word-Optionen\Sicherheit *Word Options\Security*		
11.	**Ausgeblendete Markups anzeigen** *Make hidden markups visible*	☑
12.	**Zufallszahl zur Verbesserung der Zusammenführungsgenauigkeit speichern** *Store random number to improve merge accuracy*	☒
13.	**Dateiüberprüfung deaktivieren** *Turn off file validation*	☒
14.	**Warnung anzeigen, bevor eine Datei, die Überarbeitungen oder Kommentare enthält,**	☑

1 Eingabeaufforderung

	gedruckt, gespeichert oder versendet wird *Warn before printing, saving or sending a file that contains tracked changes or comments*	
15.	**Vor der Aktualisieren der Felder „IncludePicture“ und „IncludeText“ in Word keine Genehmigung anfordern** *Don‘t ask permission before updating IncludePicture and IncludeText fields in Word*	☒

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

Word-Optionen\Sicherheit\Trust Center *Word Options\Security\Trust Center*		
26.	**Alle Anwendungs-Add-Ins deaktivieren** *Disable all application add-ins*	☒
27.	**Dynamischer Datenaustausch** *Dynamic Data Exchange*	☒
28.	**Blockieren der Ausführung von Makros in Office-Dateien aus dem Internet** *Block macros from running in Office files from the Internet*	☑
29.	**Einstellungen für VBA-Makrobenachrichtigungen** *VBA Macro Notification Settings*	☑[10]

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

30.	**Vertrauenswürdige Dokumente deaktivieren** *Turn off trusted documents*	☒
31.	**Verschlüsselte Makros in Word Open XML-Dokumenten überprüfen** *Scan encrypted macros in Word Open XML documents*	☑[11]
32.	**Anwendungs-Add-Ins müssen von einem vertrauenswürdigen Herausgeber signiert sein** *Require that application add-ins are signed by Trusted Publisher*	☑
33.	**Vertrauenswürdige Dokumente im Netzwerk deaktivieren** *Turn off Trusted Documents on the network*	☒
34.	**Zugriff auf Visual Basic-Project vertrauen** *Trust access to Visual Basic Project*	☒
35.	**Benachrichtigungen für Vertrauensstellungsleiste für nicht signierte Anwendungs-Add-Ins deaktivieren und blockieren** *Disable Trust Bar Notification for unsigned application add-ins and block them*	☑
36.	**Das Senden von eingebetteten TrueType-Schriftarten in Nachrichten zulassen** *Allow embedded TrueType fonts to be sent in messages*	☒
37.	**Maximale Anzahl beizubehaltender Vertrauenstellungs-Datensätze festlegen** *Set maximum number of trust records to preserve*	☑[12]
38.	**Maximale Anzahl vertrauenswürdiger Dokumente festlegen** *Set maximum number of trusted documents*	☑[13]

Word-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz *Word Options\Security\Trust Center\File Block Settings*		
39.	**Binärdokumente und Vorlagen im Format Word 2 und früher** *Word 2 and earlier binary documents and templates*	☑[14]
40.	**Binärdokumente und Vorlagen im Format Word 2007 und später** *Word 2007 and later binary documents and templates*	☑[15]
41.	**Dokumente und Vorlagen im Format Word 2007 und später** *Word 2007 and later documents and templates*	☑[16]
42.	**Nur-Text-Dateien** *Plain text files*	☑[17]
43.	**Office Open XML-Konverter für Word** *Office Open XML converters for Word*	☑[18]
44.	**OpenDocument-Textdateien** *OpenDocument Text files*	☑[19]
45.	**RTF-Dateien** *RTF files*	☑[20]
46.	**Standardverhalten für Zugriffsschutz festlegen** *Set default file block behavior*	☑[21]
47.	**Vorversionskonverter für Word** *Legacy converters for Word*	☑[22]

11 Verschlüsselte Makros überprüfen
12 400
13 500
14 Blockieren
15 Nicht blockieren
16 Nicht blockieren
17 Nicht blockieren
18 Nicht blockieren
19 Nicht blockieren
20 Nicht blockieren
21 Blockierte Dateien werden nicht geöffnet
22 Nicht blockieren

48.	**Webseiten** *Web pages*	☑[23]
49.	**Word 6.0-Binärdokumente und -vorlagen** *Word 6.0 binary documents and templates*	☑[24]
50.	**Word 95-Binärdokumente und -vorlagen** *Word 95 binary documents and templates*	☑[25]
51.	**Word 97-Binärdokumente und -vorlagen** *Word 97 binary documents and templates*	☑[26]
52.	**Word 2000-Binärdokumente und -vorlagen** *Word 2000 binary documents and templates*	☑[27]
53.	**Word 2003-Binärdokumente und -vorlagen** *Word 2003 binary documents and templates*	☑[28]
54.	**Word 2003- und unformatierte XML-Dokumente** *Word 2003 and plain XML documents*	☑[29]
55.	**Word XP-Binärdokumente und -vorlagen** *Word XP binary documents and templates*	☑[30]

Word-Optionen\Sicherheit\Trust Center\Geschützte Ansicht *Word Options\Security\Trust Center\Protected View*		
56.	**Dateien an unsicheren Speicherorten nicht in der geschützten Ansicht öffnen** *Do not open files in unsafe locations in Protected View*	☒
57.	**Dateien aus der Internetzone nicht in der geschützten Ansicht öffnen** *Do not open files from the Internet zone in Protected View*	☒
58.	**Dateien mit lokalem UNC-Intranetpfad in geschützter Ansicht öffnen** *Open files on local Intranet UNC in Protected View*	☒
59.	**Dokumentenverhalten bei Fehlschlagen der Dateiüberprüfung festlegen** *Set document behavior if file validation fails*	☑[31]
60.	**Geschützte Ansicht für aus Outlook geöffnete Anlagen deaktivieren** *Turn off Protected View for attachments opened from Outlook*	☒

Word-Optionen\Sicherheit\Trust Center\Vertrauenswürdige Speicherorte *Word Options\Security\Trust Center\Trusted Locations*		
61.	**Alle vertrauenswürdigen Speicherorte deaktivieren** *Disable all trusted locations*	☑
62.	**Vertrauenswürdige Speicherorte im Netzwerk zulassen** *Allow Trusted Locations on the network*	☒
63.	**Vertrauenswürdiger Speicherort #1 bis #20** *Trusted Location #1 to #20*	☒

23 Nicht blockieren
24 Blockieren
25 Blockieren
26 Nicht blockieren
27 Nicht blockieren
28 Nicht blockieren
29 Nicht blockieren
30 Nicht blockieren
31 In geschützter Ansicht öffnen und Bearbeitung nicht zulassen

Restrisiken

Die Konfiguration der Gruppenrichtlinien hilft nur dabei, die Angriffsfläche auf Anwendungen von Microsoft Word 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 gesendet werden.