



EMPFEHLUNG: IT IN UNTERNEHMEN

Sichere Konfiguration von Microsoft Excel 2013/2016/2019

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.

1 Ziel

Hauptaugenmerk dieser Empfehlung liegt auf dem Einsatz von Microsoft Excel 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 75 Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft Excel 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 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
- ✓ Sichere Konfiguration von Microsoft Word 2013/2016/2019

2 Sicherheitsprinzipien

Bei vielen Anwendungsprodukten ist die Konfiguration häufig ein Kompromiss aus Si-

cherheit 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.

3 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-Grundsatz enthaltenen Empfehlungen und bewährten Methoden implementiert wurden.

4 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. Dar-

über 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 <i>Miscellaneous</i>		
1.	OLAP PivotTable-UDF-Sicherheitseinstellung OLAP PivotTable User Defined Function (UDF) security setting	<input checked="" type="checkbox"/> ¹
2.	Alle nicht verwalteten Add-ins blockieren Block all unmanaged add-ins	<input checked="" type="checkbox"/>
3.	Liste der verwalteten Add-Ins List of managed add-ins	<input checked="" type="checkbox"/>

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

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

Datenwiederherstellung <i>Data Recovery</i>		
8.	Datenextrahierungsoptionen beim Öffnen beschädigter Arbeitsmappen nicht anzeigen Do not show data extraction options when opening corrupt workbooks	<input checked="" type="checkbox"/>

Excel-Optionen\Erweitert <i>Excel Options\Advanced</i>		
9.	Andere Anwendungen ignorieren Ignore other applications	<input checked="" type="checkbox"/>
10.	Aktualisierungen von automatischen Verknüpfungen bestätigen Ask to update automatic links	<input checked="" type="checkbox"/>

1 Nur sichere UDFs zulassen

Excel-Optionen\Erweitert\Weboptionen...\Allgemein <i>Excel Options\Advanced\Web Options...\General</i>		
11.	Bilder von Webseiten laden, die nicht mit Excel erstellt wurden Load pictures from Web pages not created in Excel	<input type="checkbox"/>

Excel-Optionen\Rechtschreibprüfung\AutoKorrektur-Optionen <i>Excel Options\Proofing\Autocorrect Options</i>		
12.	Internet- und Netzwerkpfade als Links Internet and network paths as hyperlinks	<input type="checkbox"/>

Excel-Optionen\Speichern <i>Excel Options\Save</i>		
13.	Keine Warnung bei automatischem Wiederveröffentlichen anzeigen Do not show AutoRepublish warning alert	<input type="checkbox"/>
14.	Automatisches Wiederveröffentlichen deaktivieren Disable AutoRepublish	<input checked="" type="checkbox"/>

Excel-Optionen\Sicherheit <i>Excel Options\Security</i>		
15.	Dateiüberprüfung deaktivieren Turn off file validation	<input type="checkbox"/>
16.	Übereinstimmung der Dateierweiterung mit dem Dateityp erzwingen Force file extension to match file type	<input checked="" type="checkbox"/> ²
17.	Dateiüberprüfung in PivotTable-Caches ausführen Perform file validation on pivot caches	<input checked="" type="checkbox"/> ³
18.	Benachrichtigungseinstellungen für die WEBSERVICE-Funktion WEBSERVICE Function Notification Settings	<input checked="" type="checkbox"/> ⁴
19.	Verschlüsselte Makros in Excel Open XML-Arbeitsmappen überprüfen Scan encrypted macros in Excel Open XML workbooks	<input checked="" type="checkbox"/> ⁵

Excel-Optionen\Sicherheit\Kryptografie <i>Excel Options\Security\Cryptography</i>		
20.	Algorithmus für CNG-Zufallszahlen-Generator angeben Specify CNG random number generator algorithm	<input checked="" type="checkbox"/> ⁶
21.	Anzahl für CNG-Kennwortwechsel festlegen Set CNG password spin count	<input checked="" type="checkbox"/> ⁷
22.	Bei Kennwortänderung neuen Schlüssel verwenden Use new key on password change	<input type="checkbox"/>
23.	CNG-Chiffreverkettungsmodus konfigurieren Configure CNG cipher chaining mode	<input checked="" type="checkbox"/> ⁸

2 Andere zulassen, aber warnen

3 Web- und E-Mail-Quellen

4 Alle mit Benachrichtigung deaktivieren

5 Verschlüsselte Makros überprüfen

6 RNG

7 100.000

8 CBC (Blockchiffreverkettung, Cipher Block Chaining)

24.	CNG-Chiffrieralgorithmus festlegen Set CNG cipher algorithm	<input checked="" type="checkbox"/> ⁹
25.	CNG-Hashalgorithmus angeben Specify CNG hash algorithm	<input checked="" type="checkbox"/> ¹⁰
26.	Länge des CNG-Chiffrierschlüssels festlegen Set CNG cipher key length	<input checked="" type="checkbox"/> ¹¹
27.	Länge für CNG-Salt angeben Specify CNG salt length	<input checked="" type="checkbox"/> ¹²
28.	Parameter für CNG-Kontext festlegen Set parameters for CNG context	<input type="checkbox"/>
29.	Verschlüsselungskompatibilität angeben Specify encryption compatibility	<input type="checkbox"/> ¹³

Excel-Optionen\Sicherheit\Trust Center <i>Excel Options\Security\Trust Center</i>		
30.	Alle Anwendungs-Add-Ins deaktivieren Disable all application add-ins	<input type="checkbox"/>
31.	Einstellungen für VBA-Makrobenachrichtigungen VBA Macro Notification Settings	<input checked="" type="checkbox"/> ¹⁴
32.	Vertrauenswürdige Dokumente deaktivieren Turn off trusted documents	<input type="checkbox"/>
33.	Makro standardmäßig in Persönliche Makroarbeitsmappe speichern Store macro in Personal Macro Workbook by default	<input checked="" type="checkbox"/>
34.	Anwendungs-Add-Ins müssen von einem vertrauenswürdigen Herausgeber signiert sein Require that application add-ins are signed by Trusted Publisher	<input checked="" type="checkbox"/>
35.	Vertrauenswürdige Dokumente im Netzwerk deaktivieren Turn off Trusted Documents on the network	<input type="checkbox"/>
36.	Zugriff auf Visual Basic-Project vertrauen Trust access to Visual Basic Project	<input type="checkbox"/>
37.	Benachrichtigungen für Vertrauensstellungsleiste für nicht signierte Anwendungs-Add-Ins deaktivieren und blockieren Disable Trust Bar Notification for unsigned application add-ins and block them	<input checked="" type="checkbox"/>
38.	Ausführung von Makros in Office-Dateien aus dem Internet blockieren Block macros from running in Office files from the Internet	<input checked="" type="checkbox"/>

Excel-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz <i>Excel Options\Security\Trust Center\File Block Settings</i>		
39.	Excel 2-Makrovorlagen und -Add-In-Dateien Excel 2 macrosheets and add-in files	<input checked="" type="checkbox"/> ¹⁵
40.	Excel 3-Makrovorlagen und -Add-In-Dateien Excel 3 macrosheets and add-in files	<input checked="" type="checkbox"/> ¹⁶

9 AES

10 SHA512

11 128

12 16

13 Format der nächsten Generation verwenden

14 Alle Makros außer digital signierten Makros deaktivieren

15 Blockieren

16 Blockieren

41.	Microsoft Office-Datenverbindungsdateien Microsoft Office data connection files	<input checked="" type="checkbox"/> 17
42.	Excel 95-97 Arbeitsmappen und -Vorlagen Excel 95-97 workbooks and templates	<input checked="" type="checkbox"/> 18
43.	Excel 2-Arbeitsblätter Excel 2 worksheets	<input checked="" type="checkbox"/> 19
44.	Andere Datenquellendateien Other data source files	<input checked="" type="checkbox"/> 20
45.	Excel 4-Arbeitsblätter Excel 4 worksheets	<input checked="" type="checkbox"/> 21
46.	Excel 3-Arbeitsblätter Excel 3 worksheets	<input checked="" type="checkbox"/> 22
47.	OpenDocument-Kalkulationstabellendateien OpenDocument Spreadsheet files	<input checked="" type="checkbox"/> 23
48.	Arbeitsmappen und Vorlagen im Format 2007 und später Excel 2007 and later workbooks and templates	<input checked="" type="checkbox"/> 24
49.	dBase III / IV Dateien dBase III / IV files	<input checked="" type="checkbox"/> 25
50.	Binärarbeitsmappen im Format Excel 2007 und später Excel 2007 and later binary workbooks	<input checked="" type="checkbox"/> 26
51.	Webseiten und Excel 2003-XML-Kalkulationstabellen Web pages and Excel 2003 XML spreadsheets	<input checked="" type="checkbox"/> 27
52.	Makroaktivierte Arbeitsmappen und Vorlagen im Format Excel 2007 und später Excel 2007 and later macro-enabled workbooks and templates	<input checked="" type="checkbox"/> 28
53.	Microsoft Office-Abfragedateien Microsoft Office query files	<input checked="" type="checkbox"/> 29
54.	Vorversionskonverter für Excel Legacy converters for Excel	<input checked="" type="checkbox"/> 30
55.	Excel 95-Arbeitsmappen Excel 95 workbooks	<input checked="" type="checkbox"/> 31
56.	Add-In-Dateien im Format Excel 2007 und später Excel 2007 and later add-in files	<input checked="" type="checkbox"/> 32
57.	XML Dateien XML files	<input checked="" type="checkbox"/> 33
58.	Offlinecubedateien Offline cube files	<input checked="" type="checkbox"/> 34

- 17 Nicht blockieren
- 18 Nicht blockieren
- 19 Nicht blockieren
- 20 Nicht blockieren
- 21 Nicht blockieren
- 22 Blockieren
- 23 Nicht blockieren
- 24 Nicht blockieren
- 25 Nicht blockieren
- 26 Blockieren
- 27 Nicht blockieren
- 28 Nicht blockieren
- 29 Nicht blockieren
- 30 Nicht blockieren
- 31 Nicht blockieren
- 32 Nicht blockieren
- 33 Nicht blockieren
- 34 Nicht blockieren

59.	Excel-Add-In-Dateien Excel add-in files	<input checked="" type="checkbox"/> 35
60.	Standardverhalten für Zugriffsschutz festlegen Set default file block behavior	<input checked="" type="checkbox"/> 36
61.	Textdateien Text files	<input checked="" type="checkbox"/> 37
62.	Excel 4-Makrovorlagen und -Add-In-Dateien Excel 4 macrosheets and add-in files	<input checked="" type="checkbox"/> 38
63.	Excel 97-2003-Arbeitsmappen und -Vorlagen Excel 97-2003 workbooks and templates	<input checked="" type="checkbox"/> 39
64.	Microsoft Office Open XML-Konverter für Excel Microsoft Office Open XML converters for Excel	<input checked="" type="checkbox"/> 40
65.	Excel 4-Arbeitsmappen Excel 4 workbooks	<input checked="" type="checkbox"/> 41
66.	DIF- und SYLK-Dateien Dif and Sylk files	<input checked="" type="checkbox"/> 42
67.	Excel 97-2003-Add-In-Dateien Excel 97-2003 add-in files	<input checked="" type="checkbox"/> 43

Excel-Optionen\Sicherheit\Trust Center\Geschützte Ansicht <i>Excel Options\Security\Trust Center\Protected View</i>		
68.	Dateien an unsicheren Speicherorten nicht in der geschützten Ansicht öffnen Do not open files in unsafe locations in Protected View	<input type="checkbox"/>
69.	Dateien aus der Internetzone nicht in der geschützten Ansicht öffnen Do not open files from the Internet zone in Protected View	<input type="checkbox"/>
70.	Dateien mit lokalem UNC-Intranetpfad in geschützter Ansicht öffnen Open files on local Intranet UNC in Protected View	<input type="checkbox"/>
71.	Dokumentenverhalten bei Fehlschlagen der Dateiüberprüfung festlegen Set document behavior if file validation fails	<input checked="" type="checkbox"/> 44
72.	Geschützte Ansicht für aus Outlook geöffnete Anlagen deaktivieren Turn off Protected View for attachments opened from Outlook	<input type="checkbox"/>

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

35 Nicht blockieren

37 Nicht blockieren

36 Blockierte Dateien werden nicht geöffnet

38 Nicht blockieren

39 Nicht blockieren

40 Nicht blockieren

41 Blockieren

42 Nicht blockieren

43 Nicht blockieren

44 In geschützter Ansicht öffnen und Bearbeitung nicht zulassen

5 Restrisiken

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

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 cs-info@bsi.bund.de gesendet werden.