



EMPFEHLUNG: IT IN UNTERNEHMEN

Sichere Konfiguration von Microsoft Excel

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 Excel 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 Excel.** 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 Excel, die sicherheitsrelevant sind. Weitere Einstellungen finden sich in den BSI-Veröffentlichungen:

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

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

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

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

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

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

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

1 Nur sichere UDFs zulassen

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

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

| Excel-Optionen\Sicherheit\Kryptografie <i>Excel Options\Security\Cryptography</i> | | |
|---|--|---|
| 20. | Algorithmus für CNG-Zufallszahlen-Generator angeben <i>Specify CNG random number generator algorithm</i> | <input checked="" type="checkbox"/> ⁶ |
| 21. | Anzahl für CNG-Kennwortwechsel festlegen <i>Set CNG password spin count</i> | <input checked="" type="checkbox"/> ⁷ |
| 22. | Bei Kennwortänderung neuen Schlüssel verwenden <i>Use new key on password change</i> | <input type="checkbox"/> |
| 23. | CNG-Chiffreverkettungsmodus konfigurieren <i>Configure CNG cipher chaining mode</i> | <input checked="" type="checkbox"/> ⁸ |
| 24. | CNG-Chiffrieralgorithmus festlegen <i>Set CNG cipher algorithm</i> | <input checked="" type="checkbox"/> ⁹ |
| 25. | CNG-Hashalgorithmus angeben <i>Specify CNG hash algorithm</i> | <input checked="" type="checkbox"/> ¹⁰ |
| 26. | Länge des CNG-Chiffrierschlüssels festlegen <i>Set CNG cipher key length</i> | <input checked="" type="checkbox"/> ¹¹ |
| 27. | Länge für CNG-Salt angeben <i>Specify CNG salt length</i> | <input checked="" type="checkbox"/> ¹² |
| 28. | Parameter für CNG-Kontext festlegen <i>Set parameters for CNG context</i> | <input type="checkbox"/> |

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)

9 AES

10 SHA512

11 256

12 16

| | | |
|-----|--|---|
| 29. | Verschlüsselungskompatibilität angeben <i>Specify encryption compatibility</i> | <input checked="" type="checkbox"/> ¹³ |
|-----|--|---|

| Excel-Optionen\Sicherheit\Trust Center <i>Excel Options\Security\Trust Center</i> | | |
|---|---|---|
| 30. | Alle Anwendungs-Add-Ins deaktivieren <i>Disable all application add-ins</i> | <input checked="" type="checkbox"/> |
| 31. | Einstellungen für Makrobenachrichtigungen <i>Macro Notification Settings</i> | <input checked="" type="checkbox"/> ¹⁴ |
| 32. | Vertrauenswürdige Dokumente deaktivieren <i>Turn off trusted documents</i> | <input checked="" type="checkbox"/> |
| 33. | Makro standardmäßig in Persönliche Makroarbeitsmappe speichern <i>Store macro in Personal Macro Workbook by default</i> | <input checked="" type="checkbox"/> |
| 34. | Anwendungs-Add-Ins müssen von einem vertrauenswürdigen Herausgeber signiert sein <i>Require that application add-ins are signed by Trusted Publisher</i> | <input checked="" type="checkbox"/> |
| 35. | Vertrauenswürdige Dokumente im Netzwerk deaktivieren <i>Turn off Trusted Documents on the network</i> | <input checked="" type="checkbox"/> |
| 36. | Zugriff auf Visual Basic-Project vertrauen <i>Trust access to Visual Basic Project</i> | <input checked="" type="checkbox"/> |
| 37. | Benachrichtigungen für Vertrauensstellungsleiste für nicht signierte Anwendungs-Add-Ins deaktivieren und blockieren <i>Disable Trust Bar Notification for unsigned application add-ins and block them</i> | <input checked="" type="checkbox"/> |
| 38. | Blockieren der Ausführung von Makros in Office-Dateien aus dem Internet <i>Block macros from running in Office files from the Internet</i> | <input checked="" type="checkbox"/> |
| 39. | Maximale Anzahl beizubehaltender Vertrauensstellungs-Datensätze festlegen <i>Set maximum number of trust records to preserve</i> | <input checked="" type="checkbox"/> ¹⁵ |
| 40. | Maximale Anzahl vertrauenswürdiger Dokumente festlegen <i>Set maximum number of trusted documents</i> | <input checked="" type="checkbox"/> ¹⁶ |
| 41. | Excel am Ausführen von XLM-Makros hindern <i>Prevent Excel from running XLM macros</i> | <input checked="" type="checkbox"/> |

| Excel-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz <i>Excel Options\Security\Trust Center\File Block Settings</i> | | |
|--|--|---|
| 42. | Excel 2-Makrovorlagen und -Add-In-Dateien <i>Excel 2 macrosheets and add-in files</i> | <input checked="" type="checkbox"/> ¹⁷ |
| 43. | Excel 3-Makrovorlagen und -Add-In-Dateien <i>Excel 3 macrosheets and add-in files</i> | <input checked="" type="checkbox"/> ¹⁸ |
| 44. | Microsoft Office-Datenverbindungsdateien <i>Microsoft Office data connection files</i> | <input checked="" type="checkbox"/> ¹⁹ |
| 45. | Excel 95-97 Arbeitsmappen und -Vorlagen <i>Excel 95-97 workbooks and templates</i> | <input checked="" type="checkbox"/> ²⁰ |

13 Format der nächsten Generation verwenden

14 Alle VBA-Makros außer digital signierten Makros deaktivieren

15 400

16 500

17 Blockieren

18 Blockieren

19 Nicht blockieren

20 Nicht blockieren

| | | |
|-----|--|---|
| 46. | Excel 2-Arbeitsblätter <i>Excel 2 worksheets</i> | <input checked="" type="checkbox"/> ²¹ |
| 47. | Andere Datenquellendateien <i>Other data source files</i> | <input checked="" type="checkbox"/> ²² |
| 48. | Excel 4-Arbeitsblätter <i>Excel 4 worksheets</i> | <input checked="" type="checkbox"/> ²³ |
| 49. | Excel 3-Arbeitsblätter <i>Excel 3 worksheets</i> | <input checked="" type="checkbox"/> ²⁴ |
| 50. | OpenDocument-Kalkulationstabellendateien <i>OpenDocument Spreadsheet files</i> | <input checked="" type="checkbox"/> ²⁵ |
| 51. | Arbeitsmappen und Vorlagen im Format 2007 und später <i>Excel 2007 and later workbooks and templates</i> | <input checked="" type="checkbox"/> ²⁶ |
| 52. | dBase III / IV Dateien <i>dBase III / IV files</i> | <input checked="" type="checkbox"/> ²⁷ |
| 53. | Binärarbeitsmappen im Format Excel 2007 und später <i>Excel 2007 and later binary workbooks</i> | <input checked="" type="checkbox"/> ²⁸ |
| 54. | Webseiten und Excel 2003-XML-Kalkulationstabellen <i>Web pages and Excel 2003 XML spreadsheets</i> | <input checked="" type="checkbox"/> ²⁹ |
| 55. | Makroaktivierte Arbeitsmappen und Vorlagen im Format Excel 2007 und später <i>Excel 2007 and later macro-enabled workbooks and templates</i> | <input checked="" type="checkbox"/> ³⁰ |
| 56. | Microsoft Office-Abfragedateien <i>Microsoft Office query files</i> | <input checked="" type="checkbox"/> ³¹ |
| 57. | Vorversionskonverter für Excel <i>Legacy converters for Excel</i> | <input checked="" type="checkbox"/> ³² |
| 58. | Excel 95-Arbeitsmappen <i>Excel 95 workbooks</i> | <input checked="" type="checkbox"/> ³³ |
| 59. | Add-In-Dateien im Format Excel 2007 und später <i>Excel 2007 and later add-in files</i> | <input checked="" type="checkbox"/> ³⁴ |
| 60. | XML Dateien <i>XML files</i> | <input checked="" type="checkbox"/> ³⁵ |
| 61. | Offlinecubedateien <i>Offline cube files</i> | <input checked="" type="checkbox"/> ³⁶ |
| 62. | Excel-Add-In-Dateien <i>Excel add-in files</i> | <input checked="" type="checkbox"/> ³⁷ |

21 Blockieren

24 Blockieren

23 Blockieren

22 Nicht blockieren

25 Nicht blockieren

26 Nicht 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

35 Nicht blockieren

36 Nicht blockieren

37 Nicht blockieren

| | | |
|-----|---|---|
| 63. | Standardverhalten für Zugriffsschutz festlegen <i>Set default file block behavior</i> | <input checked="" type="checkbox"/> ³⁸ |
| 64. | Textdateien <i>Text files</i> | <input checked="" type="checkbox"/> ³⁹ |
| 65. | Excel 4-Makrovorlagen und -Add-In-Dateien <i>Excel 4 macrosheets and add-in files</i> | <input checked="" type="checkbox"/> ⁴⁰ |
| 66. | Excel 97-2003-Arbeitsmappen und -Vorlagen <i>Excel 97-2003 workbooks and templates</i> | <input checked="" type="checkbox"/> ⁴¹ |
| 67. | Microsoft Office Open XML-Konverter für Excel <i>Microsoft Office Open XML converters for Excel</i> | <input checked="" type="checkbox"/> ⁴² |
| 68. | Excel 4-Arbeitsmappen <i>Excel 4 workbooks</i> | <input checked="" type="checkbox"/> ⁴³ |
| 69. | DIF- und SYLK-Dateien <i>Dif and Sylk files</i> | <input checked="" type="checkbox"/> ⁴⁴ |
| 70. | Excel 97-2003-Add-In-Dateien <i>Excel 97-2003 add-in files</i> | <input checked="" type="checkbox"/> ⁴⁵ |

| Excel-Optionen\Sicherheit\Trust Center\Geschützte Ansicht <i>Excel Options\Security\Trust Center\Protected View</i> | | |
|---|--|---|
| 71. | Dateien an unsicheren Speicherorten nicht in der geschützten Ansicht öffnen <i>Do not open files in unsafe locations in Protected View</i> | <input type="checkbox"/> |
| 72. | Keine Dateien aus der Internetzone in der geschützten Ansicht öffnen <i>Do not open files from the Internet zone in Protected View</i> | <input type="checkbox"/> |
| 73. | Dateien mit lokalem UNC-Intranetpfad in geschützter Ansicht öffnen <i>Open files on local Intranet UNC in Protected View</i> | <input type="checkbox"/> |
| 74. | Dokumentenverhalten bei Fehlschlagen der Dateiüberprüfung festlegen <i>Set document behavior if file validation fails</i> | <input checked="" type="checkbox"/> ⁴⁶ |
| 75. | Geschützte Ansicht für aus Outlook geöffnete Anlagen deaktivieren <i>Turn off Protected View for attachments opened from Outlook</i> | <input type="checkbox"/> |

| Excel-Optionen\Sicherheit\Trust Center\Vertrauenswürdige Speicherorte <i>Excel Options\Security\Trust Center\Trusted Locations</i> | | |
|--|---|-------------------------------------|
| 76. | Alle vertrauenswürdigen Speicherorte deaktivieren <i>Disable all trusted locations</i> | <input checked="" type="checkbox"/> |
| 77. | Vertrauenswürdige Speicherorte im Netzwerk zulassen <i>Allow Trusted Locations on the network</i> | <input type="checkbox"/> |
| 78. | Vertrauenswürdiger Speicherort #1 bis #20 <i>Trusted Location #1 to #20</i> | <input type="checkbox"/> |

38 Blockierte Dateien werden nicht geöffnet

39 Nicht blockieren

40 Blockieren

41 Nicht blockieren

42 Nicht blockieren

43 Blockieren

44 Nicht blockieren

45 Nicht blockieren

46 In geschützter Ansicht öffnen und Bearbeitung nicht zulassen

Restrisiken

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