Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN UNTERNEHMEN

Sichere Konfiguration von Microsoft Visio

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 Visio 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 2021von Microsoft Visio.** 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 Visio , 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 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 *Miscellaneous*		
1.	**Alle nicht verwalteten Add-ins blockieren** *Block all unmanaged add-ins*	☑
2.	**Liste der verwalteten Add-Ins** *List of managed add-ins*	☑

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

Elemente in Benutzeroberfläche deaktivieren\Vordefiniert *Disable Items in User Interface\Predefined*		
5.	**Befehle deaktivieren** *Disable commands*	☒

Visio-Optionen\Sicherheit\Trust Center *Visio Options\Security\Trust Center*		
6.	**Alle Anwendungs-Add-Ins deaktivieren** *Disable all application add-ins*	☒
7.	**Blockieren der Ausführung von Makros in Office-Dateien aus dem Internet** *Block macros from running in Office files from the Internet*	☑
8.	**Einstellungen für VBA-Makrobenachrichtigungen** *VBA Macro Notification Settings*	☑[1]
9.	**Vertrauenswürdige Dokumente deaktivieren** *Turn off trusted documents*	☒
10.	**Anwendungs-Add-Ins müssen von einem vertrauenswürdigen Herausgeber signiert sein** *Require that application add-ins are signed by Trusted Publisher*	☑
11.	**Vertrauenswürdige Dokumente im Netzwerk deaktivieren** *Turn off Trusted Documents on the network*	☒
12.	**Benachrichtigung für Vertrauensstellungsleiste für nicht signierte Anwendungs-Add-Ins deaktivieren und blockieren** *Disable Trust Bar Notification for unsigned application add-ins and block them*	☑
13.	**Alle vertrauenswürdigen Speicherorte deaktivieren** *Disable all trusted locations*	☑
14.	**Vertrauenswürdige Speicherorte im Netzwerk zulassen** *Allow Trusted Locations on the network*	☒
15.	**Vertrauenswürdiger Speicherort Nr. 1 - 20** *Trusted Location #1 - 20*	☒
16.	**Maximale Anzahl beizubehaltender Vertrauenstellungs-Datensätze festlegen** *Set maximum number of trust records to preserve*	☑[2]

1 Alle Makros außer digital signierten Makros deaktivieren
2 400

17.	**Maximale Anzahl vertrauenswürdiger Dokumente festlegen** *Set maximum number of trusted documents*	☑[3]

Visio-Optionen\Sicherheit\Trust Center\Einstellungen für den Zugriffsschutz *Visio Options\Security\Trust Center\File Block Settings*		
18.	**Binäre Visio 5.0-Zeichnungen, -Vorlagen und -Schablonen (oder früher)** *Visio 5.0 or earlier Binary Drawings, Templates and Stencils*	☑[4]
19.	**Binäre Visio 2000-2002-Zeichnungen, -Vorlagen und -Schablonen** *Visio 2000-2002 Binary Drawings, Templates and Stencils*	☑[5]
20.	**Binäre Visio 2003-2010-Zeichnungen, -Vorlagen und -Schablonen** *Visio 2003-2010 Binary Drawings, Templates and Stencils*	☑[6]

Restrisiken

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

3 500
4 Öffnen/Speichern blockiert
5 Öffnen/Speichern blockiert
6 Öffnen/Speichern blockiert