
**APP.1: Client-Anwendungen**

# APP.1.1: Office-Produkte

## 1 Beschreibung

### 1.1 Einleitung

Die Gruppe der Office-Produkte umfasst in erster Linie Anwendungen, die dazu dienen, Dokumente zu erstellen, zu bearbeiten oder zu betrachten. Dazu zählen unter anderem die freie Anwendung LibreOffice und die proprietäre Anwendung Microsoft Office, die in vielen Institutionen genutzt werden. Office-Produkte gehören für die meisten Institutionen zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme und einfache Datenbanksysteme.

### 1.2 Zielsetzung

Ziel des vorliegenden Bausteins ist der Schutz der Informationen, die durch Office-Produkte verarbeitet und genutzt werden. Dazu werden spezielle Anforderungen an die Funktionsweise der Komponenten von Office-Produkten gestellt. Der Baustein zeigt Anforderungen auf, die zur Absicherung von Office-Produkten vor spezifischen Gefährdungen erfüllt werden sollten.

### 1.3 Abgrenzung und Modellierung

Der Baustein APP.1.1 *Office-Produkte* ist auf jedes Office Produkt anzuwenden, mit dem Dokumente betrachtet, bearbeitet oder erstellt werden.

Dieser Baustein betrachtet den Einsatz von Office-Produkten aus Sicht des IT-Betriebs und gibt Hinweise für Benutzer, wie Office-Produkte eingesetzt werden sollten. Ergänzend zu den Anforderungen dieses Bausteins müssen die Anforderungen des übergeordneten Bausteins APP.6 *Allgemeine Software* umgesetzt werden. E-Mail-Anwendungen werden in diesem Baustein nicht berücksichtigt, die entsprechenden Anforderungen sind im Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* zu finden. Bei der Verwendung von integrierten Datenbanksystemen wie Base in LibreOffice oder Access in Microsoft Office muss der Baustein APP.4.3 *Relationale Datenbanksysteme* berücksichtigt werden. Ebenfalls im vorliegenden Baustein ausgenommen sind reine Cloud-Office-Anwendungen wie Googles G Suite mit den Anwendungen Docs oder Sheets. Anforderungen an Cloud-Anwendungen sind in dem Baustein OPS.2.2 *Cloud-Nutzung* festgelegt.

## 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.1.1 *Office-Produkte* von besonderer Bedeutung.

### 2.1 Fehlende Anpassung der Office-Produkte an den Bedarf der Institution

Werden Office-Produkte beschafft oder angepasst, ohne die Anforderungen an diese Software zu beachten, kann der Betrieb erheblich gestört werden. Es kann beispielsweise sein, dass vorhandene Vorlagen und Dokumente nicht kompatibel sind oder mit Anwendungen von Geschäftspartnern nicht interoperabel ist. Sollten Office-Produkte nicht an den Bedarf der Institution angepasst werden, kann dies zu Performance-Verlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

### 2.2 Schädliche Inhalte in Office-Dokumenten

Office-Dokumente können in der Regel verschiedene sogenannte „Aktive Inhalte" oder Makros enthalten, die mitunter für komplexe Automatisierungen genutzt werden. Aktive Inhalte können aber auch Schadcode enthalten, der ausgeführt wird, wenn das Dokument geöffnet wird. Solche Schadfunktionen in Office-Dokumenten können die betroffenen Dokumente selbst, aber auch andere Daten und Programme manipulieren. Darüber hinaus kann sich der Schadcode weiter ausbreiten. Alle betroffenen Geschäftsprozesse der Institution können in ihren Funktionen gestört oder blockiert werden. Im schlimmsten Fall bleibt die Manipulation unerkannt und führt zu Sicherheitslücken und zur Verarbeitung von verfälschten Informationen.

### 2.3 Integritätsverlust von Office-Dokumenten

Die Integrität von Office-Dokumenten kann verfälscht werden, wenn unbeabsichtigt oder vorsätzlich die Inhalte geändert werden. Durch einen unbedachten Umgang mit Office-Produkten oder durch Unkenntnis der Benutzer im Umgang mit Office-Dokumenten können Dokumente unerkannt geändert werden. Dies ist dann besonders problematisch, wenn es sich um produktiv eingesetzte Dokumente handelt. Wird mit Dokumenten weitergearbeitet, die unerkannt verfälscht wurden, werden möglicherweise falsche Entscheidungen getroffen oder es kann ein Image-Schaden für die Institution entstehen.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.1 *Office-Produkte* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

| **Zuständigkeiten** | **Rollen** |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Benutzer |

### 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.1 *Office-Produkte* vorrangig erfüllt werden:

**APP.1.1.A1 ENTFALLEN (B)**
Diese Anforderung ist entfallen.

**APP.1.1.A2 Einschränken von Aktiven Inhalten (B)**
Die Funktion, dass eingebettete Aktive Inhalte automatisch ausgeführt werden, MUSS deaktiviert

werden. Falls es dennoch notwendig ist, Aktive Inhalte auszuführen, MUSS darauf geachtet werden, dass Aktive Inhalte nur ausgeführt werden, wenn sie aus vertrauenswürdigen Quellen stammen. Alle Benutzer MÜSSEN hinsichtlich der Funktionen, die Aktive Inhalte einschränken, eingewiesen werden.

**APP.1.1.A3 Sicheres Öffnen von Dokumenten aus externen Quellen [Benutzer] (B)**

Alle aus externen Quellen bezogenen Dokumente MÜSSEN auf Schadsoftware überprüft werden, bevor sie geöffnet werden. Alle als problematisch eingestuften und alle innerhalb der Institution nicht benötigten Dateiformate MÜSSEN verboten werden. Falls möglich, SOLLTEN sie blockiert werden. Durch technische Maßnahmen SOLLTE erzwungen werden, dass Dokumente aus externen Quellen geprüft werden.

**APP.1.1.A4 ENTFALLEN (B)**

Diese Anforderung ist entfallen.

**APP.1.1.A17 Sensibilisierung zu spezifischen Office-Eigenschaften (B)**

Alle Benutzer MÜSSEN geeignet bezüglich der Gefährdungen durch Aktive Inhalte in Office-Dateien sensibilisiert werden. Die Benutzer MÜSSEN zum Umgang mit Dokumenten aus externen Quellen geeignet sensibilisiert werden.

Die Benutzer SOLLTEN über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert werden. Den Benutzern SOLLTE vermittelt werden, mit welchen Funktionen sie Dokumente vor nachträglicher Veränderung und Bearbeitung schützen können.

Benutzer SOLLTEN im Umgang mit den Verschlüsselungsfunktionen in Office-Produkten sensibilisiert werden.

## 3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.1.1 *Office-Produkte*. Sie SOLLTEN grundsätzlich erfüllt werden.

**APP.1.1.A5 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**APP.1.1.A6 Testen neuer Versionen von Office-Produkten (S)**

Neue Versionen von Office-Produkten SOLLTEN vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln wie Makros, Dokumentenvorlagen oder Formularen der Institution geprüft werden (Siehe hierzu *OPS.1.1.6 Software-Tests und -Freigaben).* Es SOLLTE sichergestellt sein, dass wichtige Arbeitsmittel auch mit der neuen Software-Version einwandfrei funktionieren. Bei entdeckten Inkompatibilitäten SOLLTEN geeignete Lösungen für die betroffenen Arbeitsmittel gefunden werden.

**APP.1.1.A7 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**APP.1.1.A8 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**APP.1.1.A9 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

**APP.1.1.A10 Regelung der Software-Entwicklung durch Endbenutzer (S)**

Für die Software-Entwicklung auf Basis von Office-Anwendungen, z. B. mit Makros, SOLLTEN verbindliche Regelungen getroffen werden (siehe auch APP.1.1.A2 *Einschränken von Aktiven Inhalten)*. Zunächst SOLLTE in jeder Institution die Grundsatzentscheidung getroffen werden, ob solche Eigenentwicklungen von Endbenutzern überhaupt erwünscht sind. Die Entscheidung SOLLTE in den betroffenen Sicherheitsrichtlinien dokumentiert werden. Werden Eigenentwicklungen erlaubt, SOLLTE

ein Verfahren für den Umgang mit entsprechenden Funktionen der Office-Produkte für die Endbenutzer erstellt werden. Zuständigkeiten SOLLTEN klar definiert werden. Alle Informationen über die erstellten Anwendungen SOLLTEN dokumentiert werden. Aktuelle Versionen der Regelungen SOLLTEN allen betroffenen Benutzern zeitnah zugänglich gemacht und von diesen beachtet werden.

### APP.1.1.A11 Geregelter Einsatz von Erweiterungen für Office-Produkte (S)

Alle Erweiterungen von Office-Produkten, wie Add-ons und Extensions, SOLLTEN vor dem produktiven Einsatz genauso getestet werden wie neue Versionen. Hierbei SOLLTE ausschließlich auf isolierten Testsystemen getestet werden. Die Tests SOLLTEN prüfen, ob Erweiterungen negativen Auswirkungen auf die Office-Produkte und die laufenden IT-Systeme haben. Die Tests der eingesetzten Erweiterungen SOLLTEN einem definierten Testplan folgen. Dieser Testplan SOLLTE so gestaltet sein, dass Dritte das Vorgehen nachvollziehen können.

### APP.1.1.A12 Verzicht auf Cloud-Speicherung [Benutzer] (S)

Die in einigen Office-Produkten integrierten Funktionen für Cloud-Speicher SOLLTEN grundsätzlich deaktiviert werden. Alle Cloud-Laufwerke SOLLTEN deaktiviert werden. Alle Dokumente SOLLTEN durch die Benutzer auf zentral verwalteten Fileservern der Institution gespeichert werden. Um Dokumente für Dritte freizugeben, SOLLTEN spezialisierte Anwendungen eingesetzt werden. Diese Anwendungen SOLLTEN mindestens über eine verschlüsselte Datenablage und -versendung sowie ein geeignetes System zur Benutzer- und Rechteverwaltung verfügen.

### APP.1.1.A13 Verwendung von Viewer-Funktionen [Benutzer] (S)

Daten aus potenziell unsicheren Quellen SOLLTEN automatisch in einem geschützten Modus geöffnet werden. Diese Funktion SOLLTE NICHT durch den Benutzer deaktivierbar sein. Eine Liste vertrauenswürdiger Quellen SOLLTE definiert werden, von denen Inhalte unmittelbar geöffnet und bearbeitet werden können.

In dem geschützten Modus SOLLTEN Daten NICHT unmittelbar bearbeitet werden können. Aktive Inhalte, wie Makros und Skripte, SOLLTEN im geschützten Modus NICHT automatisch ausgeführt werden. Nur eine allgemeine Navigation SOLLTE ermöglicht werden. Wenn die Dokumente lediglich betrachtet werden sollen, SOLLTEN entsprechende Viewer-Anwendungen verwendet werden, wenn diese verfügbar sind.

### APP.1.1.A14 Schutz gegen nachträgliche Veränderungen von Dokumenten [Benutzer] (S)

Je nach geplantem Verwendungszweck von Dokumenten SOLLTEN Dokumente geeignet gegen nachträgliche Veränderung geschützt werden.

## 3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.1.1 *Office-Produkte* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

### APP.1.1.A15 Einsatz von Verschlüsselung und Digitalen Signaturen (H)

Daten mit erhöhtem Schutzbedarf SOLLTEN nur verschlüsselt gespeichert bzw. übertragen werden. Bevor ein in ein Office-Produkt integriertes Verschlüsselungsverfahren genutzt wird, SOLLTE geprüft werden, ob es einen ausreichenden Schutz bietet. Zusätzlich SOLLTE ein Verfahren eingesetzt werden, mit dem Makros und Dokumente digital signiert werden können.

### APP.1.1.A16 Integritätsprüfung von Dokumenten (H)

Wenn Daten mit erhöhtem Schutzbedarf gespeichert oder übertragen werden, SOLLTEN geeignete Verfahren zur Integritätsprüfung eingesetzt werden. Falls Daten vor Manipulation geschützt werden sollen, SOLLTEN darüber hinaus kryptografische Verfahren eingesetzt werden.

# 4 Weiterführende Informationen

## 4.1 Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ folgende Dokumente zur sicheren Konfiguration von Microsoft Office 2013/2016/2019 veröffentlicht:

- BSI-CS 135: Sichere Konfiguration von Microsoft Office 2013/2016/2019
- BSI-CS 136: Sichere Konfiguration von Microsoft Excel 2013/2016/2019
- BSI-CS 137: Sichere Konfiguration von Microsoft PowerPoint 2013/2016/2019
- BSI-CS 138: Sichere Konfiguration von Microsoft Word 2013/2016/2019
- BSI-CS 139: Sichere Konfiguration von Microsoft Outlook 2013/2016/2019
- BSI-CS 140: Sichere Konfiguration von Microsoft Access 2013/2016/2019
- BSI-CS 141: Sichere Konfiguration von Microsoft Visio 2013/2016/2019

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A, A.9.4 System and application access control & A.12.5 Control of operational Software Vorgaben, die auf den Betrieb von Office-Produkten zutreffen.

# 5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.1.1 *Office-Produkte* von Bedeutung.

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.37 Abstreiten von Handlungen

G 0.39 Schadprogramme

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen