

Auf allen Dokumenten und Dateien in den klassischen Formaten sind neben den sichtbaren Elementen sogenannte Metadaten im Hintergrund gespeichert. Diese Restinformationen sind für den Nutzer auf den ersten Blick unsichtbar, können aber vertrauliche oder sensible Informationen enthalten.

Unter Metadaten versteht man Dokumenteigenschaften, die eine Datei näher beschreiben oder näher definieren. Sie sind zusätzlich zu den sichtbaren Inhalten der Datei enthalten.

Typische Beispiele:

- Namen der Autoren oder Lizenznehmer
- Datum und Ersteller der letzten Änderung
- Stichworte und Schlagworte über den Inhalt
- Informationen über vorhergehende Versionen von Dokumenten oder „gelöschte Kommentare“

Das Problem:

Diese Metadaten entstehen in der Regel automatisch und meist ohne Kenntnis des Nutzers. Sie können auch vertrauliche Informationen enthalten, die Dritten nicht zugänglich gemacht werden dürfen. Außerdem lassen sie sich beliebig erweitern.



Das betrifft praktisch alle von Ihnen genutzten klassischen Dateiformate:

- *.pdf (Adobe Portable Document Format)
- *.jpg (JPEG-Bilddatei)
- *.docx (MS Word-Textdokument)
- *.pptx (MS Power-Point-Präsentation)
- *.xlsx (MS Excel-Tabelle)

Unsichtbare Begleiter:

Warum Sie sich um die Metadaten Ihrer Dokumente kümmern müssen und wie Sie das am besten bewerkstelligen



Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©sebra (Titel), ©CalíCirilo (S. 5), ©NicoElNino (innen oben), ©James Thew (innen unten)
Text und Layout:
Rogge GmbH, Weimar



Risiken bei der ungeprüften Weitergabe von Metadaten:

Verlust der Vertraulichkeit

Mit den Metadaten können sensible Informationen unbeabsichtigt an Dritte weitergeleitet werden, die diese nicht bekommen dürfen.

Verfälschung der Restinformation

Die Metadaten in bearbeitbaren Dokumenten können vom Empfänger manipuliert werden.

Unbeabsichtigter Verstoß gegen Gesetze

Die Weitergabe schützenswerter Daten ist nach der Datenschutzverordnung des Freistaats Thüringen verboten. Das gilt auch für den Fall, dass diese Informationen nicht absichtlich weitergeleitet worden sind.

Schädigung der Behörde

Die Preisgabe sensibler Daten auf diesem Weg kann erhebliche negative Folgen für die Reputation der Behörde oder für das Ansehen einzelner Bediensteter haben.

Die Übermittlung von Metadaten macht das Behördennetzwerk angreifbar für das sogenannte Social Engineering.

Auch die Metadaten der weitergegebenen Dokumente und Dateien müssen konsequent gemanagt werden. Dafür gibt es klare Regeln und Handlungsanleitungen.

„Werden Dokumente an Dritte weitergegeben, sollten zuvor alle nicht benötigten und alle vertraulichen Restinformationen aus Office-Dokumenten entfernt werden. Zusätzlich sollten die Metadaten bereinigt werden. Dokumente sollten in einem nicht veränderbaren Format übermittelt werden, wenn keine Bearbeitung durch den Empfänger erforderlich ist.“

5 Regeln zum Sichern der Metadaten:

Vorsichtig sein

Verzichten Sie auf jede Preisgabe möglicherweise schützenswerter persönlicher Daten als Metadaten.

Prüfen und Löschen

Entfernen Sie grundsätzlich alle nicht benötigten Angaben aus den Metadaten.

Das Dokument sichern

Versenden Sie Ihre Dokumente an Dritte in einem nicht veränderlichen Format (zum Beispiel *.pdf).

Metadaten möglichst nicht erweitern

Fügen Sie den Metadaten nur dann weitere Informationen hinzu, wenn es dienstlich absolut notwendig ist.

Lückenloses Metadatenmanagement

Achten Sie auf die Minimierung der Übersendung von Metadaten auch beim Mailverkehr, bei der Übersendung von Fotos und bei der Speicherung von Dokumenten auf mobilen Speicherplätzen.



Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/ IT-Sicherheitsbeauftragte(r):

Name:

Dienst-
stelle:

Telefon:

E-Mail:

