

Sicherheit für Dateien

1.4.1 Die Auswirkung von aktivierten und deaktivierten Makro-Sicherheitseinstellungen verstehen

Makros sind automatisierte Abfolgen von Befehlen, die in Anwendungen wie Microsoft Excel oder Word verwendet werden, um wiederkehrende Aufgaben zu vereinfachen. Sie können jedoch auch Sicherheitsrisiken darstellen, insbesondere wenn sie aus unsicheren Quellen stammen.

Aktivierte Makros: Wenn Makros aktiviert sind, können sie automatisch ausgeführt werden, was die Produktivität erhöht. Allerdings besteht auch die Gefahr, dass schadhafter Code ausgeführt wird, der das System infizieren oder Daten stehlen kann.

- **Risiko:** Schadhafte Makros können Malware enthalten, die das System schädigt oder Informationen an Dritte sendet.

Deaktivierte Makros: Wenn Makros deaktiviert sind, werden sie nicht ausgeführt, was die Sicherheit erhöht, jedoch auch die Funktionalität einschränken kann.

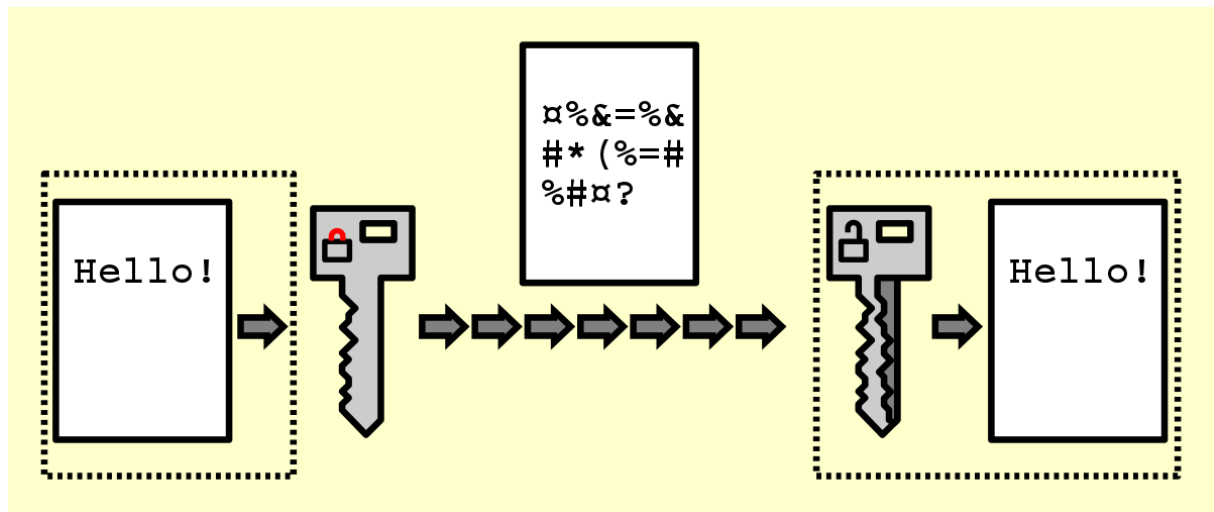
- **Vorteil:** Der Schutz vor Malware und unautorisierten Zugriffen ist höher, da potenziell gefährliche Makros nicht automatisch ausgeführt werden.



Empfehlung: Es ist ratsam, die Makro-Sicherheitseinstellungen auf "Deaktiviert" oder "Benachrichtigen", um ein gewisses Maß an Kontrolle zu haben. Nutzer sollten nur Makros aus vertrauenswürdigen Quellen aktivieren.

1.4.2 Die Vorteile und die Grenzen von Verschlüsselung verstehen

Verschlüsselung ist ein Verfahren, bei dem Informationen in eine unleserliche Form umgewandelt werden, die nur mit einem speziellen Schlüssel oder Passwort wieder entschlüsselt werden kann.



Vorteile:

- **Sicherheit der Daten:** Verschlüsselung schützt vertrauliche Informationen vor unbefugtem Zugriff, selbst wenn sie in die falschen Hände geraten.
- **Datenschutz:** Sie gewährleistet den Schutz personenbezogener Daten, was besonders wichtig ist, um Identitätsdiebstahl und Datenmissbrauch zu verhindern.

Grenzen:

- **Verlust des Schlüssels oder Passworts:** Wenn der Schlüssel oder das Passwort verloren geht, können die verschlüsselten Daten nicht mehr wiederhergestellt werden.
- **Rechenaufwand:** Die Verschlüsselung und Entschlüsselung von Daten benötigt zusätzliche Rechenleistung, was die Systemleistung beeinträchtigen kann.
- **Wichtigkeit der Geheimhaltung:** Es ist von entscheidender Bedeutung, Passwörter, Schlüssel und Zertifikate geheim zu halten, da ihr Verlust oder ihre Offenlegung zu einem vollständigen Verlust der Datenintegrität führen kann. Nur autorisierte Personen sollten Zugang zu diesen Informationen haben.

1.4.3 Eine Datei, einen Ordner oder ein Laufwerk verschlüsseln

Die Verschlüsselung von Dateien, Ordnern oder Laufwerken ist eine effektive Methode, um Daten zu schützen. Hier sind die grundlegenden Schritte zur Verschlüsselung:

Datei oder Ordner auswählen: Wählen Sie die Datei oder den Ordner aus, den Sie verschlüsseln möchten.

Verschlüsselungssoftware verwenden: Nutzen Sie geeignete Software oder integrierte Funktionen in Betriebssystemen, um die Verschlüsselung zu aktivieren.

Beispiele sind:

- Windows BitLocker für Laufwerke.
- VeraCrypt oder AxCrypt für Dateien und Ordner.

Passwort oder Schlüssel festlegen: Legen Sie ein sicheres Passwort oder einen Schlüssel für die Verschlüsselung fest. Stellen Sie sicher, dass es stark und schwer zu erraten ist.



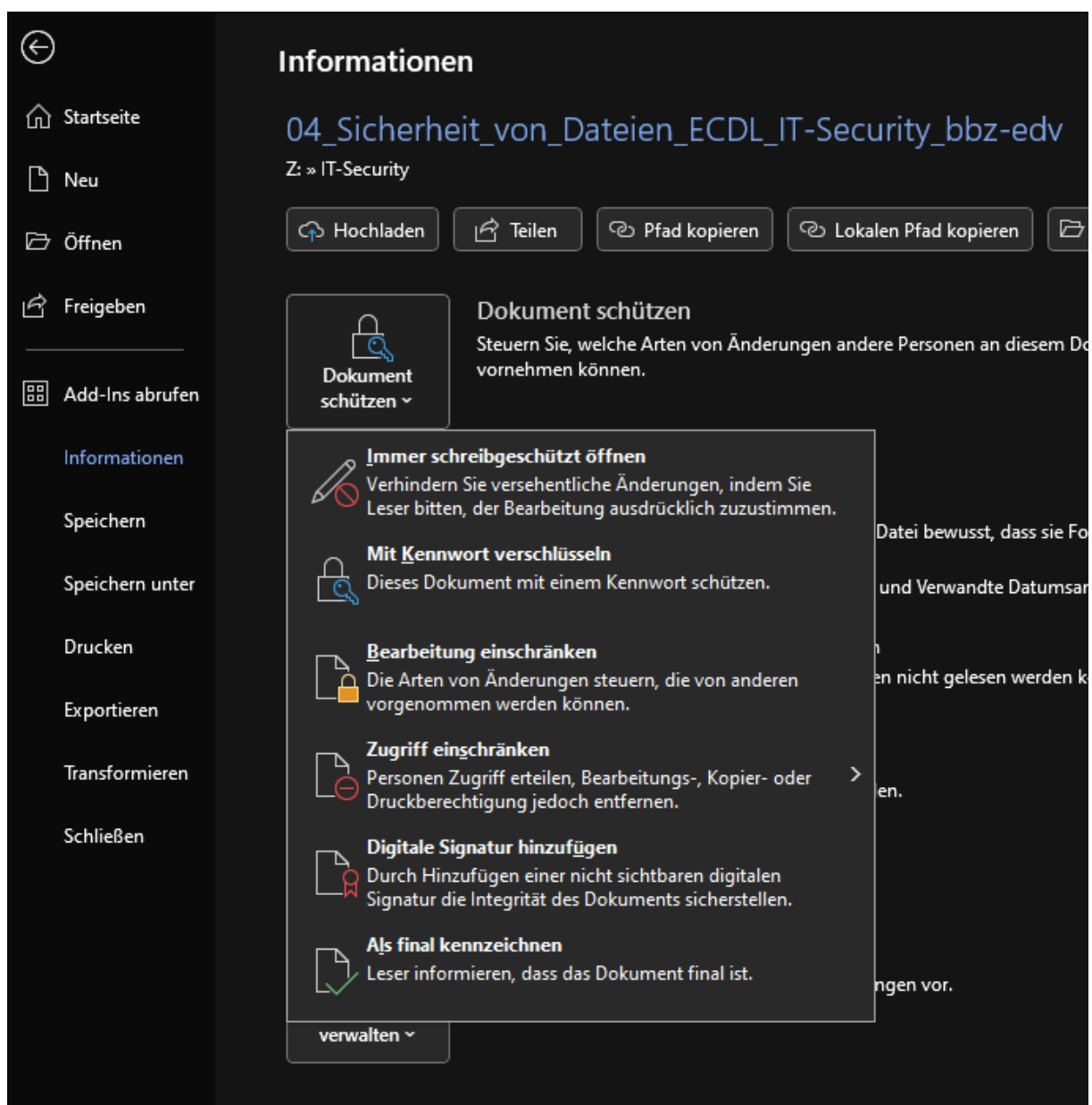
Verschlüsselung durchführen: Führe Sie die Verschlüsselung durch, indem Sie den Anweisungen der Software folgen. Nach Abschluss ist die Datei oder der Ordner geschützt und kann nur mit dem richtigen Passwort oder Schlüssel geöffnet werden.

1.4.4 Dateien mit einem Passwort schützen

Der Passwortschutz ist eine einfache und effektive Möglichkeit, um Dateien zu sichern. Hier sind die Schritte, um Dokumente, Tabellenkalkulationsdateien und komprimierte Dateien mit einem Passwort zu schützen:

Dokumente (z. B. Word, Excel):

- Öffnen Sie das Dokument.
- Gehen Sie zu den „Datei“-Informationen und wählen Sie „Dokument schützen“ oder „mit Kennwort verschlüsseln“ – Screenshot aus MS-Word.
- Geben Sie ein starkes Passwort ein und speichern Sie das Dokument.



Komprimierte Dateien bzw. Archive (z. B. ZIP-Dateien):

- Erstellen Sie eine ZIP-Datei mit dem gewünschten Inhalt.
- Verwenden Sie ein Programm wie WinRAR oder 7-Zip, das die Möglichkeit bietet, Passwörter hinzuzufügen.
- Wählen Sie beim Erstellen der ZIP-Datei die Option zum Hinzufügen eines Passworts und geben Sie ein sicheres Passwort ein.

Hinweis: Stellen Sie sicher, dass Sie das Passwort sicher aufbewahren, da der Zugriff auf die Datei ohne das richtige Passwort nicht möglich ist.