MYDATA Control

Office-Add-Ins

Veröffentlichungsdatum: 28.10.2025

Ausgabe 1

Revision 0

Inhaltsverzeichnis

1 Revisionsindex

Version	Datum der letzten Änderung	Änderung	Autor
1.0	28.10.2025	Erstversion	Jahn

2 MYDATA Control Office-Plugins

Die MYDATA Office Plugins wurden entwickelt, um Unternehmen dabei zu unterstützen, Datenverluste zu verhindern. Die – meist unbeabsichtigte – Offenlegung sensibler Informationen ist eine ständige Bedrohung für Unternehmen. Diese wird oft durch die Unachtsamkeit von Mitarbeitern und nicht durch Hacker oder böswillige Absichten verursacht.

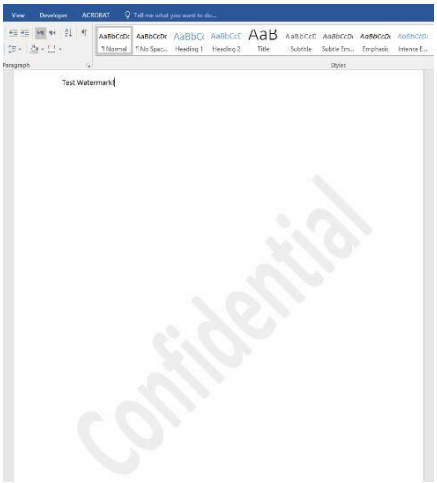
Ein Mitarbeiter versendet eine E-Mail an externe Empfänger und hat versehentlich ein vertrauliches, internes Office-Dokument angehängt. Um solche Szenarien zu verhindern, bieten die MYDATA Control Office Plugins geeignete Lösungen. Office-Dokumente (Word, Excel und PowerPoint) können nach ihrer Vertraulichkeitsstufe klassifiziert und ihre Verwendung kontrolliert werden. Wenn beispielsweise Anhänge per E-Mail versendet werden, überwacht MYDATA, dass interne Dokumente nur nach ausdrücklicher Bestätigung an externe Empfänger versendet werden. Vertrauliche Dokumente dürfen nur nach einer Verschlüsselung versendet werden. MYDATA verhindert so unerwünschte Datenlecks.

2.1 Klassifizierungs-Plugins (Word, Excel, PowerPoint)

Diese Plugins unterstützen Sie bei der Klassifizierung Ihrer Unternehmens- und

persönlichen Dokumente. Wir haben vier Dokumentklassen definiert:

1. **Vertraulich**: Diese Informationen sind nur für eine begrenzte Anzahl von Personen bestimmt. Bei Verlust, Missbrauch oder unbefugter Verwendung dieser Informationen kann der Schaden erheblich sein. Wenn Sie diese Dateien als „Vertraulich" klassifizieren, wird den Dateinamen der Suffix „_vertraulich" hinzugefügt. Wenn Sie sie ausdrucken möchten, wird Ihrer Datei ein Wasserzeichen hinzugefügt. (Dieses kann auf Wunsch entfernt werden.)

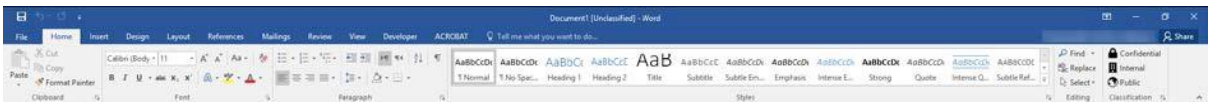


2. **Intern**: Diese Informationen sind nur für einen begrenzten Personenkreis bestimmt (in der Regel Ihre Mitarbeiter, möglicherweise auch externe Mitarbeiter), die namentlich genannt werden müssen, sofern dies nicht aus dem Kontext hervorgeht. Bei Verlust, Missbrauch oder unbefugter Verwendung dieser Informationen sind die Schäden begrenzt und überschaubar. Wenn Sie diese Dateien als „Intern" klassifizieren, wird kein Suffix an die Dateinamen angehängt.
3. **Öffentlich**: Hierbei handelt es sich um Informationen, die bereits veröffentlicht wurden, zur Veröffentlichung bestimmt sind oder deren unbeabsichtigte Veröffentlichung keinen Schaden verursachen würde. Wenn Sie diese Dateien als „öffentlich" klassifizieren, wird den Dateinamen das Suffix „_public" hinzugefügt.
4. **Persönlich**: Diese Informationen sind nur für den persönlichen Gebrauch bestimmt. In einigen Unternehmen dürfen die Mitarbeiter ihre Geräte sowohl für private als auch für geschäftliche Zwecke nutzen. Sie müssen beim Umgang mit ihren Dokumenten besonders achtsam sein. Die unbeabsichtigte Veröffentlichung dieser Dateien verursacht zwar keinen Schaden für das Unternehmen, dennoch ist es besser, ihre persönlichen Dateien als „Persönlich" zu klassifizieren, um eine Vermischung mit Arbeitsdokumenten zu vermeiden.

Wenn Sie diese Dateien als „Persönlich“ klassifizieren, wird den Dateinamen das Suffix „_personal“ hinzugefügt.

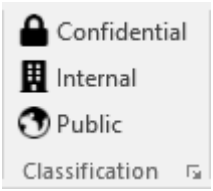
2.1.1 Klassifizierung

Sie können das Dokument über die Registerkarte „Klassifizierung“ in der Registerkarte „Start“ klassifizieren.

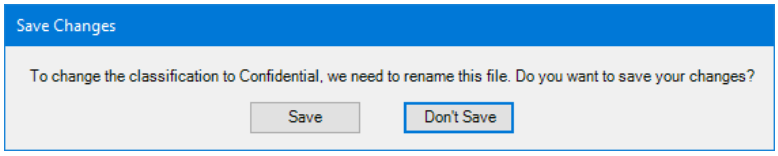


Sie können auf eine der verfügbaren Optionen klicken, um Ihr Dokument zu klassifizieren.

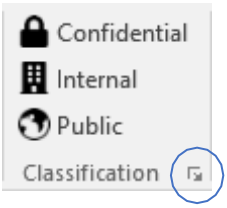
Wenn Sie die Klassifizierung „Vertraulich“ oder „Öffentlich“ wählen, müssen Sie Ihr Dokument mit den entsprechenden Suffixen umbenennen. Das Plugin fordert Sie dann auf, Ihr Dokument zu speichern. Wenn Sie „Intern“ wählen,

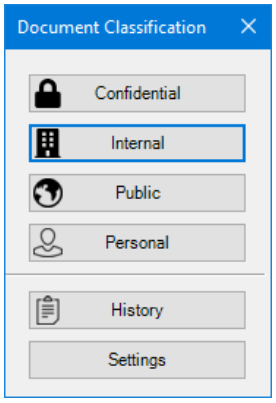


erhalten Sie diese Meldung nicht. Die Klassifizierung wird jedes Mal gespeichert, wenn Sie Ihr Dokument speichern.



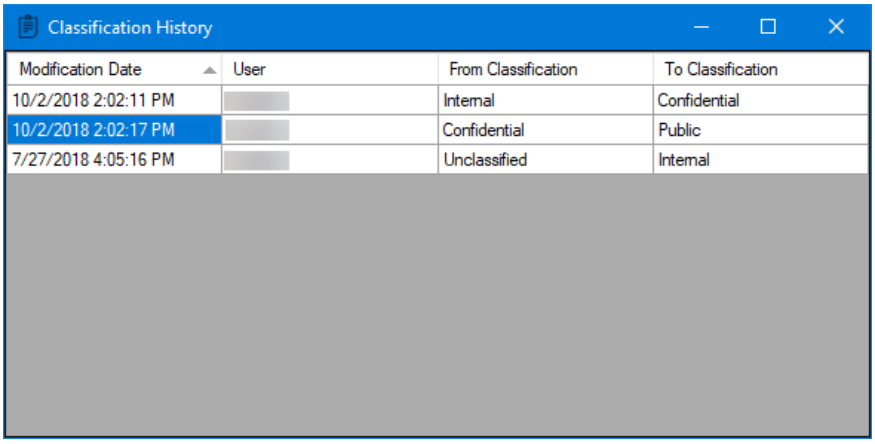
Wenn Sie das Dokument als „Persönlich“ klassifizieren, den Klassifizierungsverlauf anzeigen oder einige Einstellungen ändern möchten, klicken Sie auf den Pfeil für erweiterte Optionen.





2.1.2 Klassifizierungsverlauf

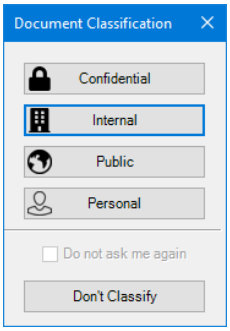
Wenn Sie auf die Schaltfläche „Verlauf“ klicken, können Sie den Verlauf der Dateiklassifizierung anzeigen. Im folgenden Beispiel sehen Sie, dass am 02.10.2018 um 14:02:17 Uhr die Klassifizierung des entsprechenden Dokuments von „Vertraulich“ in „Öffentlich“ geändert wurde. Dies wird für zukünftige Zwecke protokolliert!


Classification History
Modification Date
User
From Classification
To Classification
10/2/2018 2:02:11 PM
Internal
Confidential
10/2/2018 2:02:17 PM
Confidential
Public
7/27/2018 4:05:16 PM
Unclassified
Internal

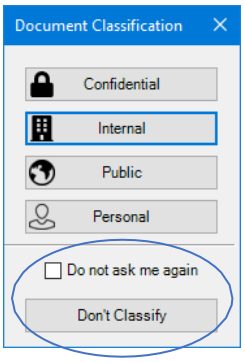
2.1.3 Blacklisting

Beim Schließen eines Dokuments

Wenn Sie ein Dokument schließen möchten, das noch nicht klassifiziert ist, werden Sie aufgefordert, es zu klassifizieren. Sie haben auch die Möglichkeit, dieses bestimmte Dokument „nicht zu klassifizieren".



Wenn es sich um ein bereits gespeichertes Dokument handelt, das nicht klassifiziert ist, können Sie es auf die schwarze Liste setzen, indem Sie das Kontrollkästchen „Nicht erneut fragen" aktivieren. Wenn Sie nun auf die Schaltfläche „Nicht klassifizieren" klicken, wird die Datei nicht klassifiziert und beim nächsten Öffnen der Datei wird keine weitere Aufforderung zur Klassifizierung angezeigt.

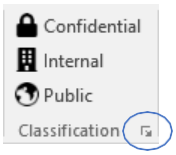


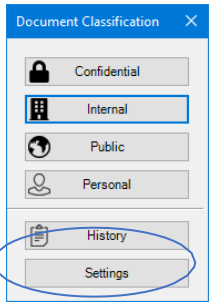
2.1.4 Einstellungen

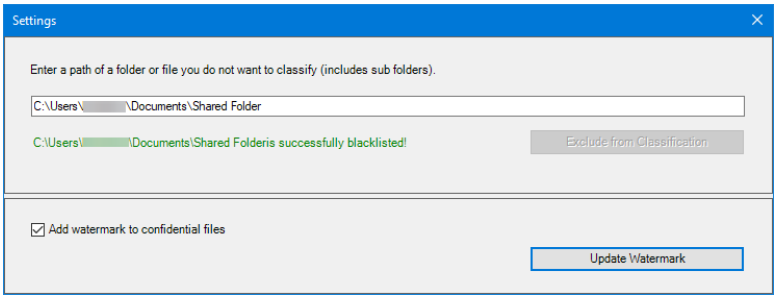
Wenn Sie auf die Schaltfläche „Einstellungen" klicken, haben Sie die Möglichkeit, neue Dateien oder Verzeichnisse zur Blacklist hinzuzufügen. Darüber hinaus können Sie festlegen, ob Sie Ihren Dateien beim Drucken ein vertrauliches Wasserzeichen hinzufügen möchten oder nicht.

2.1.4.1 Blacklist

Sie können auch ein Verzeichnis von der Klassifizierung ausschließen.





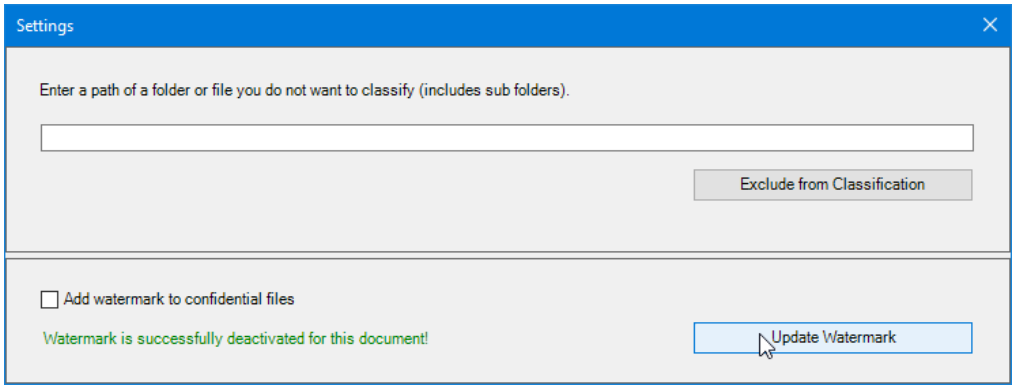


In diesem Fall werden alle Ordner und Dokumente, die in diesem Verzeichnis vorhanden sind, auf die Blacklist gesetzt. Das bedeutet, dass Sie nicht jedes Mal, wenn Sie diese Dateien schließen, aufgefordert werden, eine Klassifizierung für sie festzulegen. Um ein gesamtes Verzeichnis auf die Blacklist zu setzen, können Sie das Verzeichnis in das Textfeld einfügen und auf „Von der Klassifizierung ausschließen" klicken.

Die Blacklist (Dateien und Ordner) wird in der folgenden Datei verwaltet:
C:\Users\<User>\AppData\Local\Microsoft\Office\Office_Path_BlackList.txt

2.1.4.2 *Wasserzeichen*

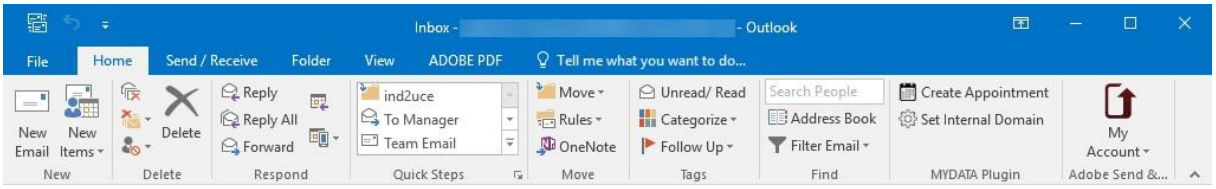
Wie bereits erwähnt, wird beim Drucken eines „vertraulichen“ Dokuments ein Wasserzeichen zu Ihrer Datei hinzugefügt. Um dieses vertrauliche Wasserzeichen zu entfernen, müssen Sie lediglich das Häkchen im Kontrollkästchen „Wasserzeichen“ entfernen und auf „Wasserzeichen aktualisieren“



klicken.

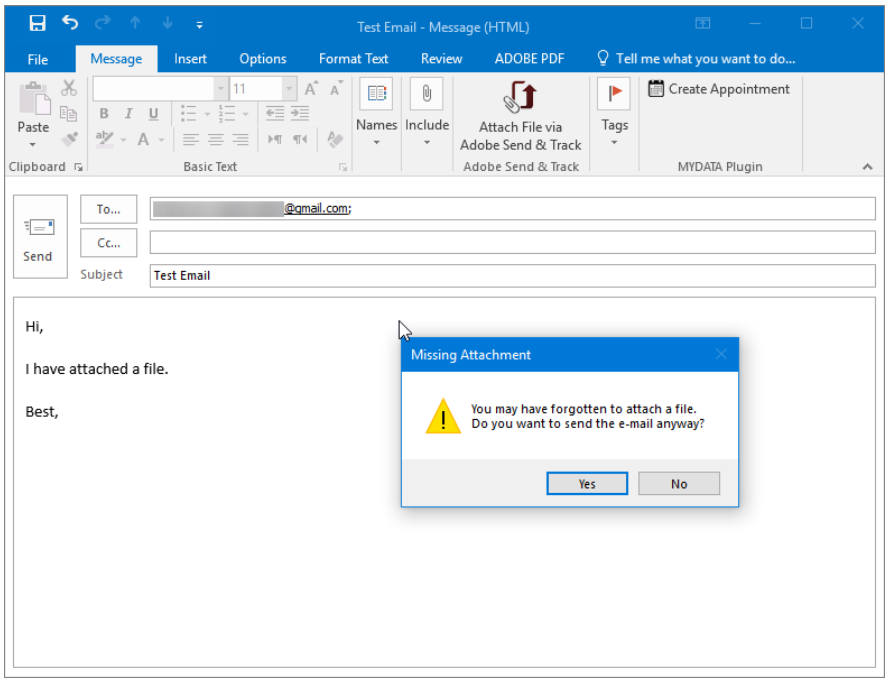
2.2 Outlook-Plugin

Das Outlook-Plugin ist in der Multifunktionsleiste „MYDATA Plugin“ auf der Registerkarte „Start“ verfügbar. Es warnt Sie, wenn Sie vertrauliche Dokumente an externe Empfänger senden, und bietet Ihnen bei Bedarf die Möglichkeit, diese zu schützen. Darüber hinaus bietet es einige praktische Funktionen, z. B. die Benachrichtigung, wenn Sie vergessen haben, eine Datei anzuhängen.



2.2.1 Fehlende Anhänge

Sie erhalten Warnungen bei fehlenden Anhängen. Dies funktioniert auf Basis einer Stichwortsuche.



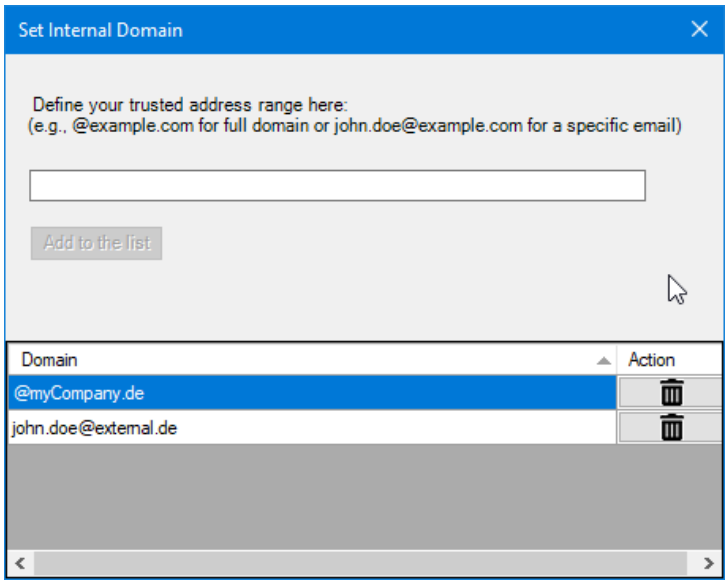
2.2.2 Große Anzahl von Empfängern

Sie erhalten Warnungen, wenn Sie E-Mails an mehr als 25 Empfänger senden.

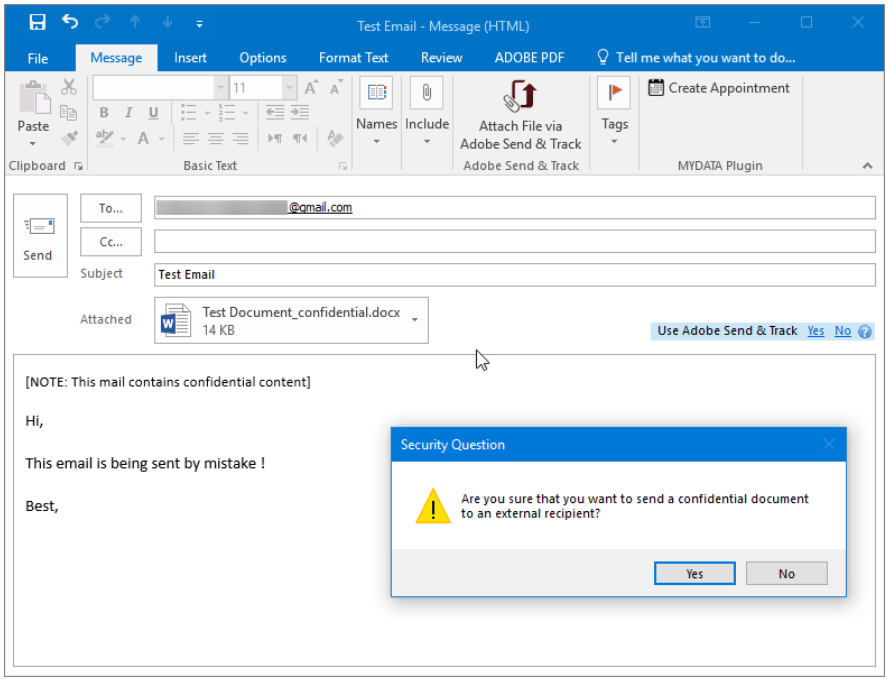
2.2.3 Warnung bei vertraulichen Anhängen

Wenn Sie versehentlich eine vertrauliche oder interne Datei an externe Empfänger senden, erhalten Sie eine Warnmeldung. Zunächst müssen Sie jedoch Ihre interne Domain definieren. Empfänger, die nicht zur internen Domain gehören, werden als externe Empfänger betrachtet.

Sie können beispielsweise „@myCompany.de“ als interne Domain festlegen. Zusätzlich können Sie „john.doe@external.de “ als vertrauenswürdige Person außerhalb Ihres Unternehmens zu Ihrer internen Domain hinzufügen.

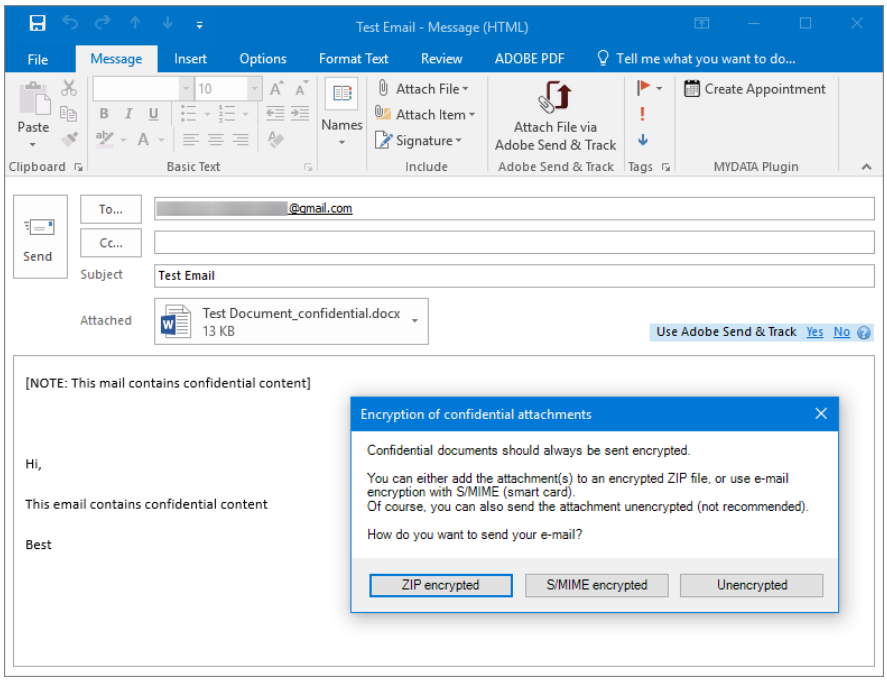


Wenn Sie ein vertrauliches Dokument an eine E-Mail anhängen, die nicht in Ihrer internen Domäne liegt, erhalten Sie eine Warnmeldung. Zusätzlich wird dem Inhalt Ihrer E-Mail ein Hinweis hinzugefügt.



2.2.4 Verschlüsselung vertraulicher Anhänge

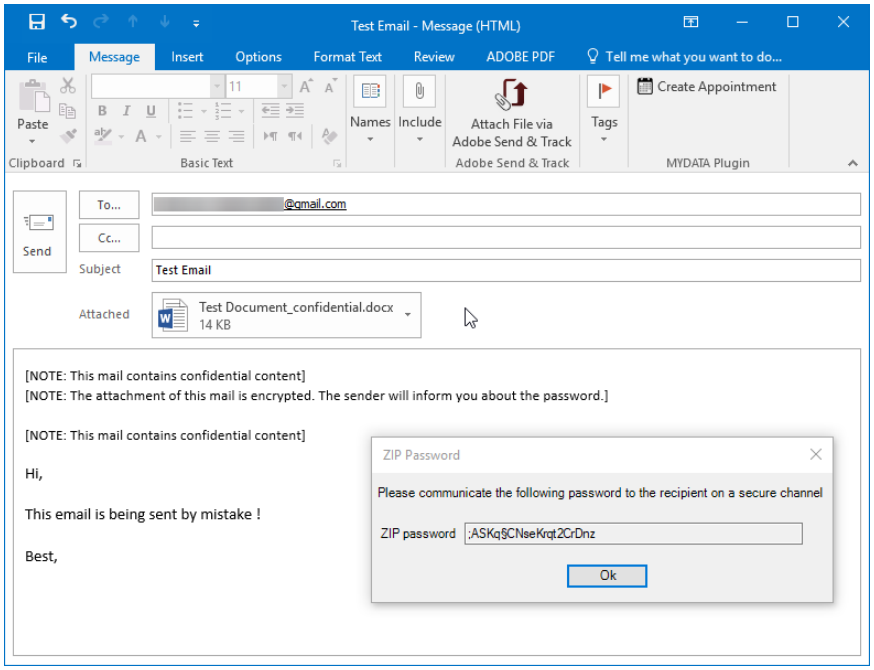
Wenn Sie eine vertrauliche Datei an einen externen Empfänger senden möchten, bietet Ihnen das Plugin die Möglichkeit, den Anhang über S/MIME oder ZIP zu verschlüsseln.



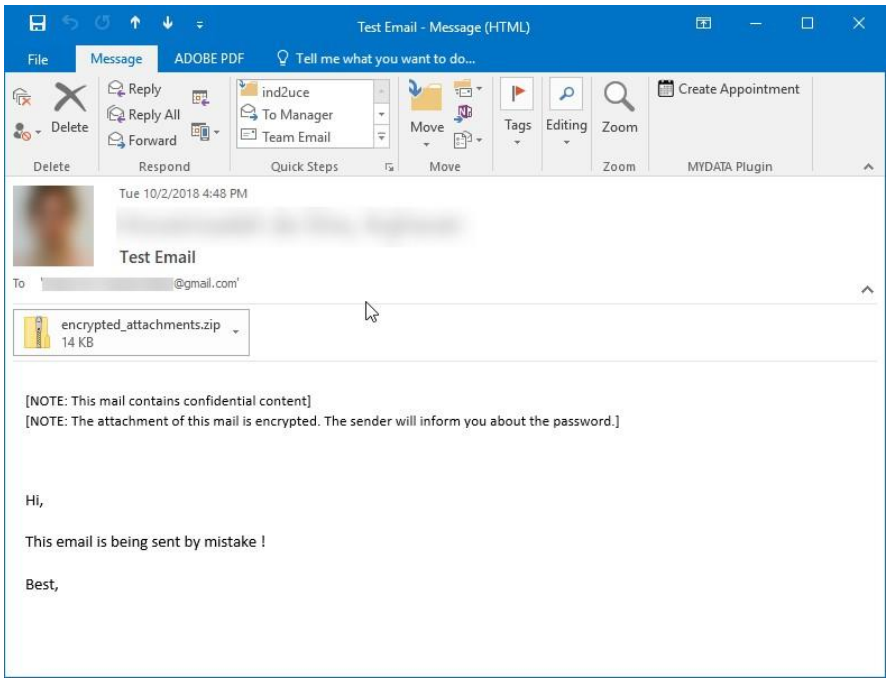
Wenn Sie sich für S/MIME entscheiden, benötigen Sie die Smartcard Ihres Unternehmens und müssen das Zertifikat des Empfängers kennen. Verfügt der Empfänger nicht über ein Zertifikat, zeigt Outlook eine Warnung an.

Sie können wählen, ob Sie die E-Mail unverschlüsselt oder mit einer ZIP-Verschlüsselung versenden möchten.

Wenn Sie sich für die ZIP-Verschlüsselung entscheiden, werden die Anhänge gezippt und verschlüsselt. Sie können das Passwort kopieren und es den Empfängern über einen sicheren/separaten Kanal zusenden. In dieser Version stellen wir nur das Passwort zur Verfügung, wie Sie in der folgenden Abbildung sehen können. Vergessen Sie nicht, das Passwort zu kopieren.



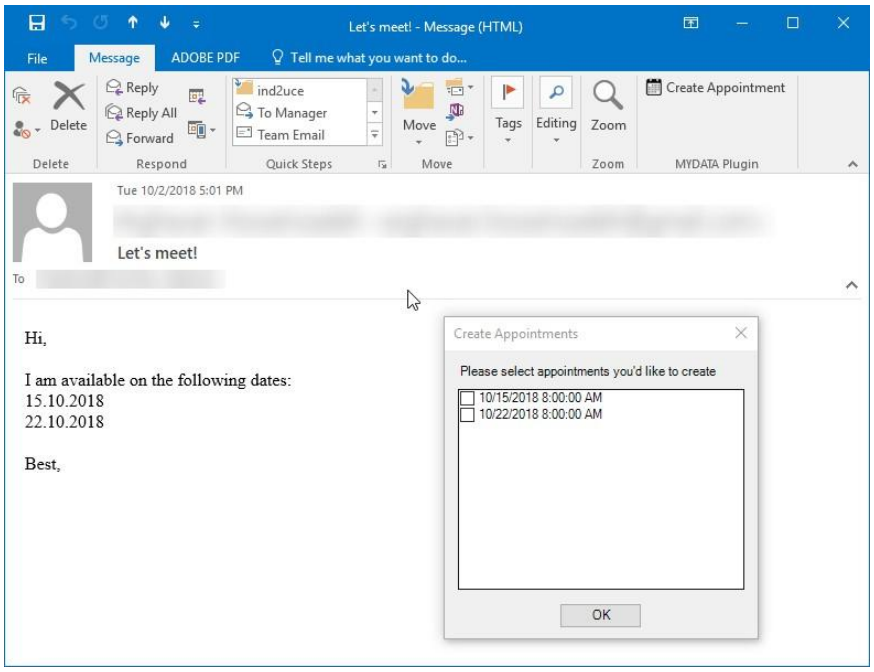
So sieht die von Ihnen gesendete E-Mail aus:



2.2.5 Automatische Terminerstellung

Sie können auf die Schaltfläche „Termin erstellen” klicken, um einen Termin an einem Datum zu erstellen, das im Inhalt einer E-Mail angegeben ist. Wenn die E-Mail mehr als ein mögliches Datum enthält, wird ein Auswahldialogfeld angezeigt.

Es ist auch möglich, ein Datum zu markieren, mit der rechten Maustaste darauf zu klicken und dann die Option „Termin erstellen“ auszuwählen.



2.3 Deinstallation

Sie können alle MYDATA-Plugins ähnlich wie alle Microsoft Office-Plugins deaktivieren oder entfernen.

Wenn Sie die Plugins von Ihrem Computer deinstallieren möchten, können Sie dies über „Programme und Funktionen“ tun. Sie können auch die Datei „unins000.exe“ aus dem Verzeichnis ausführen, in dem das Paket installiert ist:

C:\Benutzer\<Benutzer>\AppData\Local\MYDATA Office Plugin\uninstall\unins000.exe

3 Kontakt

Mail: support@lze-innovation.de

Tel.: +49 9131 92894 80

LZE GmbH

Frauenweiher Str. 15

91058 Erlangen

Viel Spaß!