Die folgenden Schulungseinheiten wurden innerhalb des vom **Bundesministerium für Wirtschaft und Energie** im Rahmen der **Initiative IT-Sicherheit in der Wirtschaft** geförderten Projekts **KMU Aware** entwickelt.

Gefördert durch:

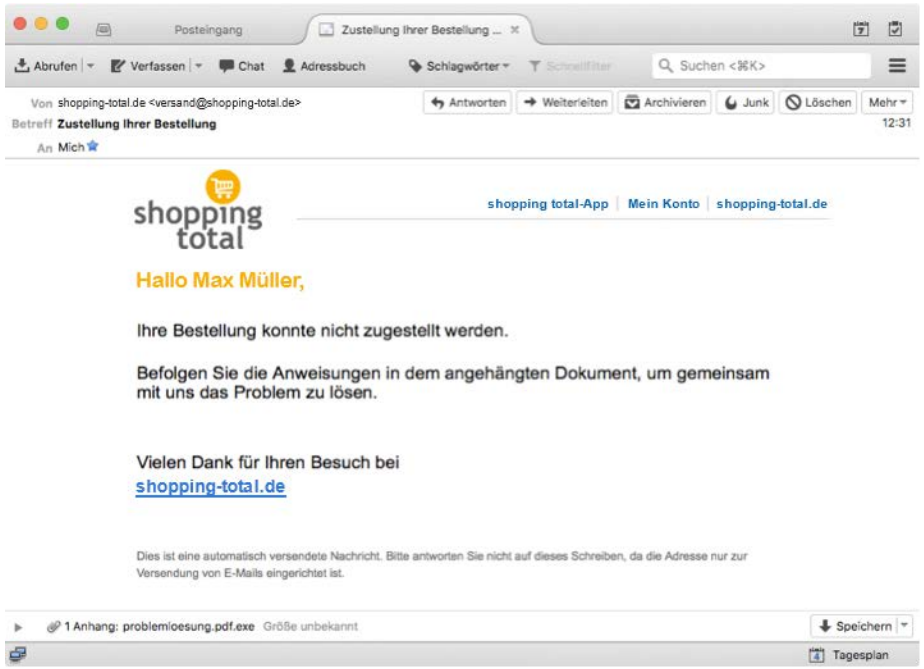
Bundesministerium
für Wirtschaft
und Energie

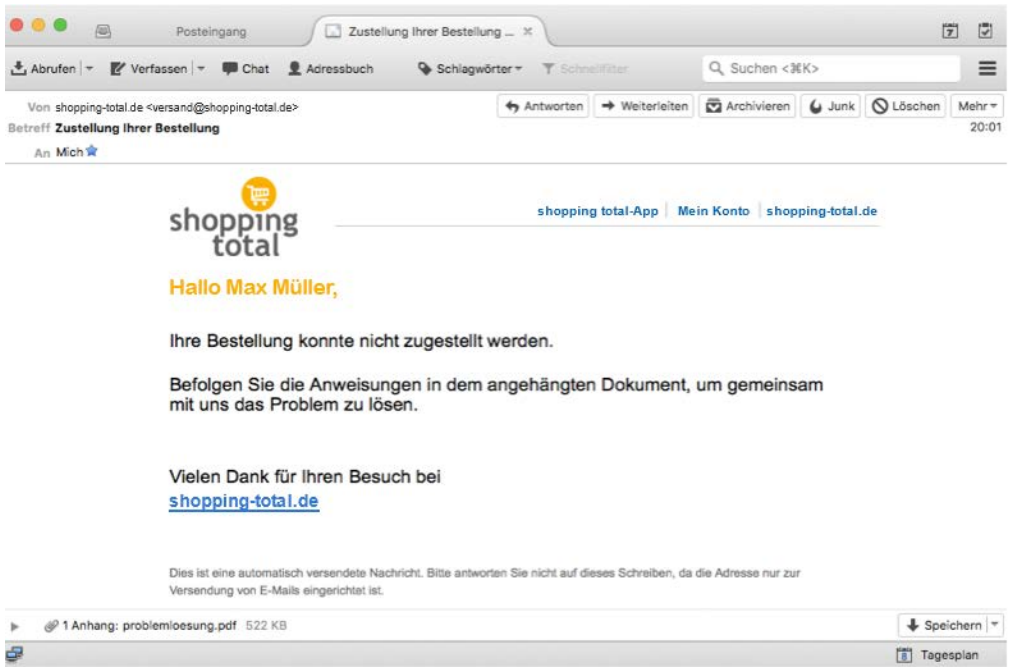
aufgrund eines Beschlusses
des Deutschen Bundestages

KMU AWARE
AWARENESS IM MITTELSTAND

IT-Sicherheit
IN DER WIRTSCHAFT

Modul 4: Erkennung von Nachrichten mit gefährlichen Anhängen





Welche Nachricht ist die gefährliche Nachricht?
Im Folgenden lernen Sie, diese und andere Nachrichten zu beurteilen.

Modul 4: Erkennung von Nachrichten mit gefährlichen Anhängen

Aufbau

1. Anleitung 1 zur Erkennung von gefährlichen Anhängen
2. Anleitung 2 zur Erkennung von gefährlichen Anhängen
3. Anleitung 3 zur Erkennung von gefährlichen Anhängen

   Alle drei Abschnitte sind in folgende Bereiche unterteilt
   a. Erklärung der Anleitung
   b. Beispiele
   c. Strategie der Betrüger, die die Erkennung erschweren
   d. Weitere Beispiele

4. Weiterführende Informationen

Wenn Absender und Inhalt einer Nachricht plausibel erscheinen und die Nachricht einen Anhang enthält, identifizieren Sie die Gefährlichkeit des Anhangs.

Anhänge in Nachrichten haben in der Regel einen Namen (z.B. rechnung) – vorderer Teil der Anhangsbezeichnung – und ein **Format** (z.B. pdf) – hinterer Teil der Anhangsbezeichnung – und werden in der Regel separat vom Text der Nachricht geführt.

Das Format des Anhangs gibt Ihnen Aufschluss über die Gefährlichkeit des Anhangs. Haben Sie

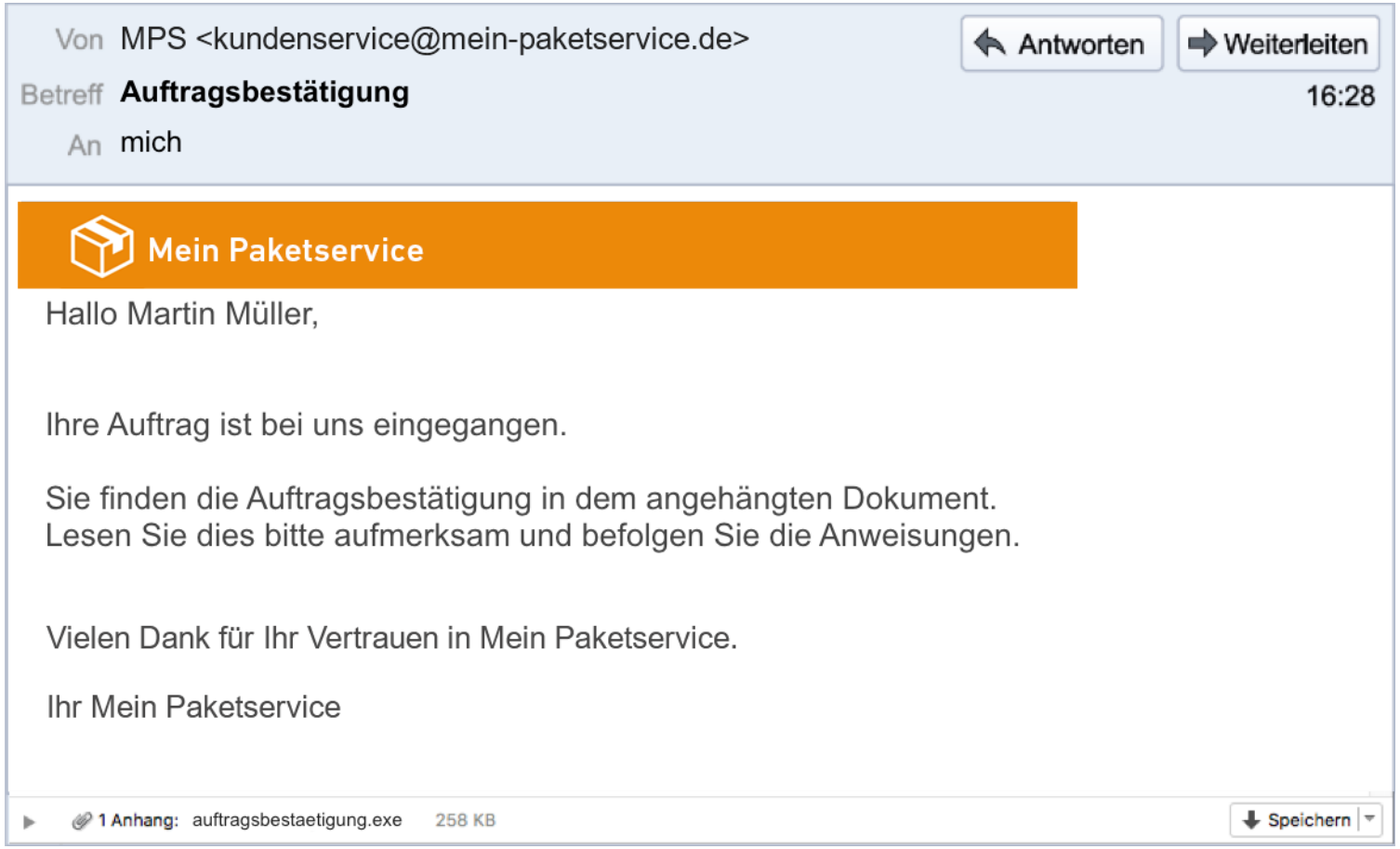
- einen direkt ausführbaren Anhang (z.B. Formate .exe, .bat, .com, .cmd, .scr, .pif) oder
- einen Anhang, der möglicherweise Makros ausführen kann (z.B. Microsoft Office Dateien wie z.B. Formate .doc, .docx, .ppt, .pptx, .xls, .xlsx), empfangen,

so ist dieser Anhang zunächst als potentiell gefährlich einzustufen. Ist Ihnen das Format eines Anhangs gänzlich unbekannt, so gehen Sie zunächst von einem potentiell gefährlichen Format aus, d.h. einem Format, das möglicherweise Schadsoftware beinhalten kann.

Einige Dienstanbieter (z.B. Webversion von Gmail) zeigen Ihnen lediglich den Namen, nicht jedoch das Format. Dort kann z.B. das Führen des Mauszeigers über den Anhang helfen den Namen und das Format des Anhangs zu erkennen.

Im Folgenden bezeichnen wir Anhänge, die ein gefährliches Format haben als gefährliche Anhänge.

Beispiel für einen Anhang mit gefährlichem Format:



Strategie der Betrüger, mit der sie Ihnen das Erkennen potentiell gefährlicher Anhänge erschweren

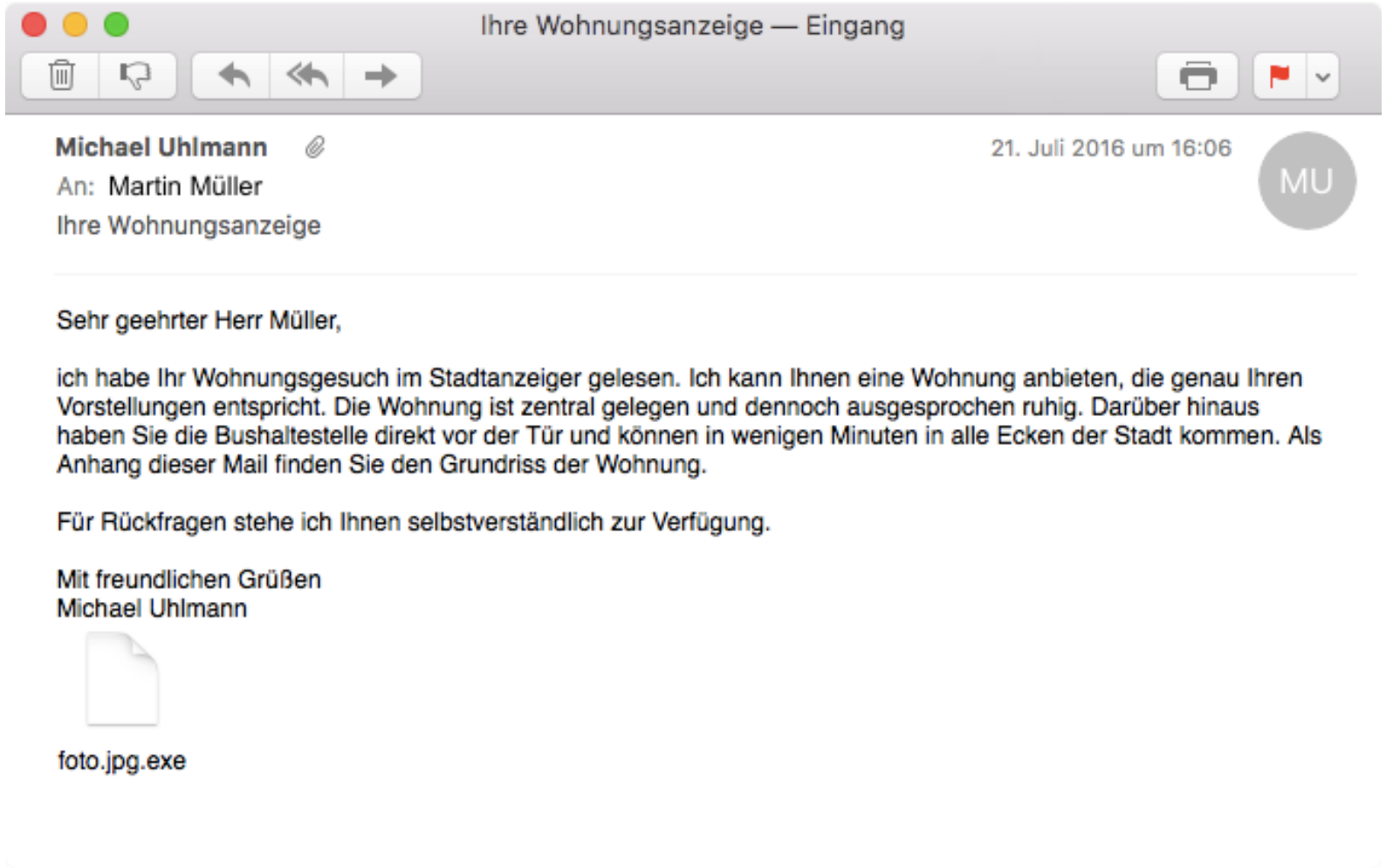
Betrüger erschweren Ihnen die Erkennung potentiell gefährlicher Anhänge, indem sie die Dateien in zunächst weniger gefährlichen Dateien verpacken. Zum Beispiel komprimieren sie Dateien und weisen ihnen dadurch z.B. die Endung **.zip** oder **.rar** zu, oder sie belegen die komprimierten Dateien gar mit einem Zugriffsschutz und lassen Ihnen das Passwort in einer Nachricht zukommen. Das Dekomprimieren kann ausgesprochen gefährlich werden, da bestimmte Dekomprimierungsprogramme den Inhalt direkt nach dem Dekomprimieren ausführen.

Beispiel für eine Strategie, mit der Betrüger Ihnen das Erkennen potentiell gefährlicher Anhänge erschweren

Weitere Strategie der Betrüger, mit der sie Ihnen das Erkennen potentiell gefährlicher Anhänge erschweren

Betrüger erschweren Ihnen die Erkennung potentiell gefährlicher Anhänge, indem sie Anhängen zwei Endungen geben (z.B. .txt.exe). Somit täuschen sie ihrem potentiellen Opfer vor einen Anhang mit ungefährlichen Format zu senden (im Beispiel eine Textdatei .txt), wobei das eigentliche Format des Anhangs z.B. .exe ist und somit direkt ausführbar ist. In diesem Beispiel wäre folglich das Öffnen des Anhangs wahrscheinlich gefährlich.

Beispiel für eine Strategie, mit der Betrüger Ihnen das Erkennen potentiell gefährlicher Anhänge erschweren



Wenn der Anhang ein potentiell gefährliches Format hat, prüfen Sie, ob Sie diesen Anhang genau in der Form von dem Absender erwarten.

Manchmal ist das Öffnen eines potentiell gefährlichen Anhangs möglich, da dessen Ungefährlichkeit aufgrund anderer Gegebenheiten als sicher gelten kann.

Zur Überprüfung, ob ein potentiell gefährlicher Anhang geöffnet werden darf, helfen Ihnen folgende Überprüfungen:

- Wurde Ihnen dieser Anhang in dieser Form zuvor von dem Absender persönlich angekündigt?
- Ist die Nachricht digital signiert, so dass die Identität des Absenders als gesichert gelten kann?

Im Zweifelsfall können Ihnen die Empfehlungen der folgenden Folien weiterhelfen.

Sollten Sie unsicher sein, ob der Anhang ein potentiell gefährliches Format hat oder ob Sie den Anhang in dieser Form vom Absender erwarten, dann sollten Sie weitere Informationen einholen bzw. weitere Maßnahmen ergreifen.

Wenn Sie bei der Beurteilung von Anhängen unsicher sind, also ob der Anhang potentiell gefährlich ist oder Sie diesen Anhang genau in dieser Form erwarten, dann können folgende Ansätze helfen:

- Kontaktieren Sie den Anbieter bzw. die Person über die Ihnen bekannten Kontaktmöglichkeiten. Insbesondere bei Ihnen bekannten Anbietern ist es wichtig, diese über Kontaktdaten zu kontaktieren, die Sie nicht direkt der Nachricht mit möglicherweise potentiell gefährlichen Inhalten entnehmen. Bitten Sie den Absender zum Beispiel, Ihnen den Anhang in einem anderen Format zu schicken, z.B. als reinen Text (.txt) oder wenn als Text nicht möglich z.B. als PDF. Betrüger, die ihre Nachrichten im großen Stil verschicken, werden sich oftmals nicht die Arbeit machen, ihren Angriff auf ein anderes Format zu übertragen.

- Suchen Sie nach dem Absender und dem Inhalt der Nachricht mit Hilfe einer Suchmaschine, z.B. Google. Bringen die ersten Suchergebnisse diese Nachricht mit Betrug in Verbindung, so sollten Sie den Anhang nicht öffnen.

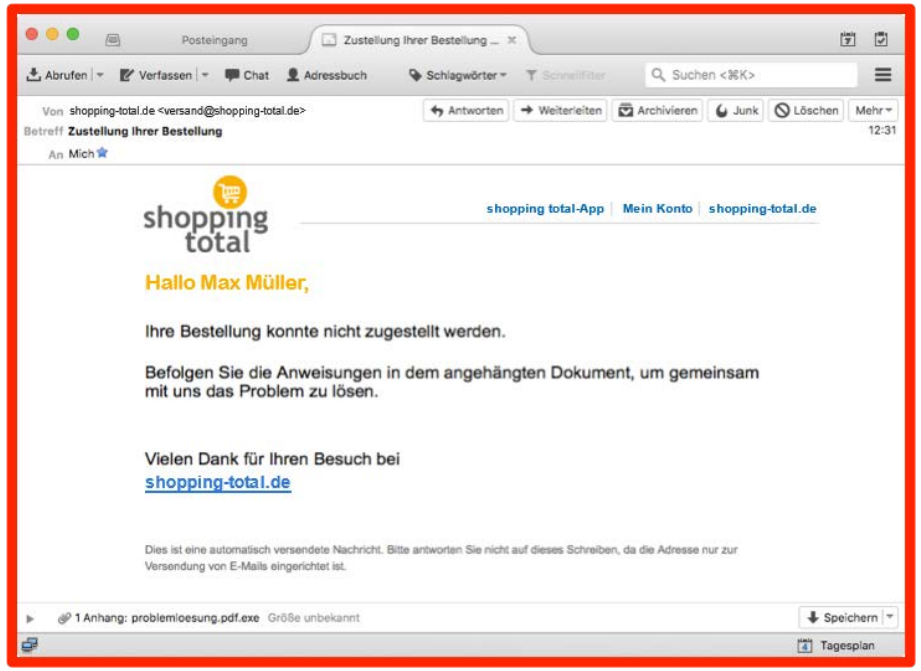
- Besprechen Sie das weitere Vorgehen mit der IT-Abteilung bzw. den IT-Verantwortlichen / IT-Experten Ihres Unternehmens oder fragen Sie bei einer Verbraucherschutzzentrale nach. Ihre IT-Abteilung bzw. die IT-Verantwortlichen / IT-Experten haben in der Regel die Möglichkeit den empfangenen Anhang manuell auf sein Schadenspotenzial zu überprüfen.

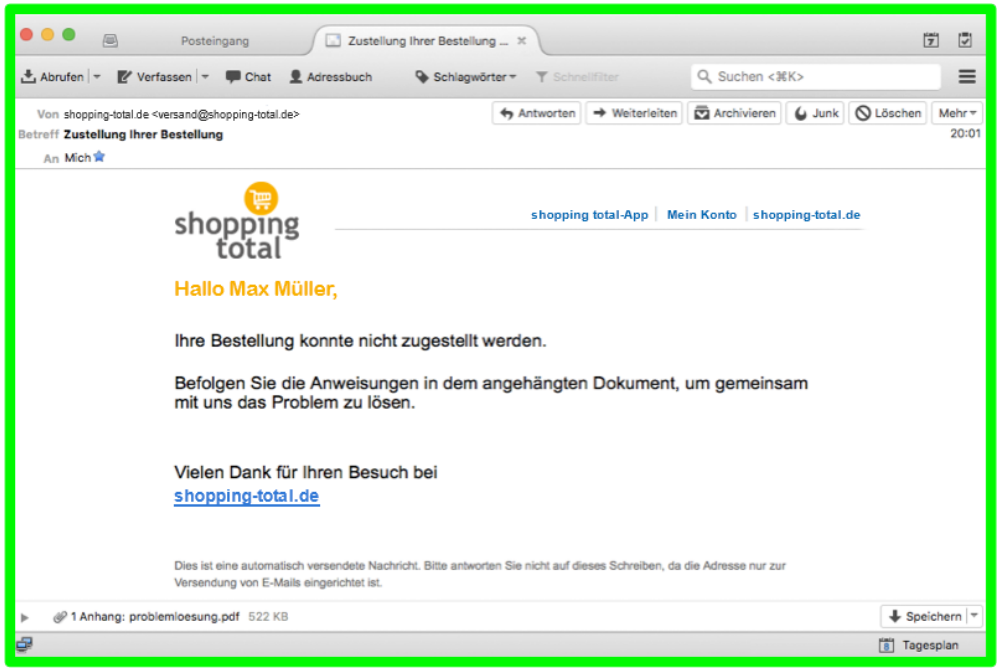
Weiterführende Informationen:

Wir möchten Ihnen abschließend noch einige weiterführende Informationen im Umgang mit Dateianhängen geben:

- Eine Übersicht über als potentiell gefährlich angesehene Formate finden Sie (in englischer Sprache) unter: http://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows/
- Oftmals werden Bild- oder Dokumentanhänge in Nachrichten automatisch angezeigt. Um dies zu vermeiden, und somit mögliche Schwachstellen zu schließen, sollten Sie – sofern möglich – das automatische Anzeigen von Anhängen unterbinden.
- Auch wenn Betrüger gezielt Doppelendungen einsetzen, um ihre Opfer in die Irre zu führen, ist zu beachten, dass Doppelendungen nicht immer auf potentiell gefährliche Anhänge hinweisen. So gibt es zum Beispiel Software, die untereinander bekannten Nutzern ermöglicht, Nachrichten und Anhänge zu verschlüsseln. Dabei wird häufig die Endung .asc an die eigentliche Datei angehängt, so dass auch dort eine Doppelendung entsteht.
- Es existieren technische Lösungen, die es Ihnen ermöglichen Anhänge in einer abgeschotteten Umgebung auf Ihrem Gerät auszuführen, ein sogenannter Sandkasten-Bereich. Anhänge können diesen Bereich nicht verlassen und können keine bleibenden Änderungen an Ihrem Gerät durchführen. Eine weit verbreitete technische Lösung, die Ihnen dies erlaubt, ist Sandboxie (http://www.sandboxie.com)
- Darüber hinaus gibt es spezielle Betriebssysteme, die z.B. von CD starten (sogenannte Live-Systeme) und somit keine Änderungen an Ihrem Gerät vornehmen können. Es kann sinnvoll sein ein derartiges Live-System einsatzbereit zu haben und im Zweifelsfall Anhänge, bei denen man sich nicht sicher ist, aus diesem Live-System heraus zu öffnen. Ein bekanntes Live-System ist Knoppix (https://www.knopper.net/knoppix/). Dieses System kann kostenlos bezogen werden.

Modul 4: Erkennung von Nachrichten mit gefährlichen Anhängen





Am Ende dieses vierten Moduls ist der Unterschied nun sicher klar.