## Zu der aktuellen Bedrohung durch Verschlüsselungstrojanern (z.B. „Locky“, „Cryptowall“)

Es gibt momentan drei gängige Wege, wie sogenannte Verschlüsselungstrojaner („Ransomware“) Ihr Netzwerk infizieren können:

1.) Sie erhalten „klassisch“ einen Virus (eigentlich: „Wurm“) z.B. als ZIP-Datei im Anhang einer Mail, worin der Benutzer aufgefordert wird, den Anhang zu öffnen. Sollten Sie das tun, wird der Virus direkt aktiv und verbreitet sich an alle Leute, mit denen Sie E-Mail-Kontakt hatten weiter. Alternativ erfolgt die Verbreitung auch direkt über Sicherheitslücken in verschiedenen Programmen.

2.) Sie erhalten z.B. eine Word- oder Exceldatei als Anhang. Oftmals von lokalen Unternehmen und in der Mail wird der Anhang als Lieferschein, Angebot, Rechnung etc. benannt. Neuerdings erfolgt das auch als E-Mail einer Privatperson mit einer vermeintlichen Bewerbung im Anhang.

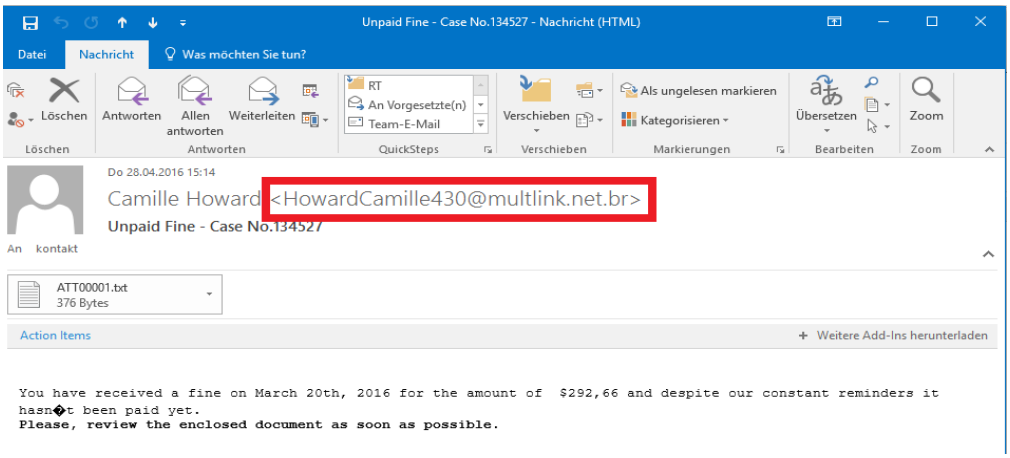
3.) Sie erhalten eine Mail, die an sich erstmal keinen Virus enthält. Es wird dann über aktive Elemente entweder direkt in der Mail oder im Anhang (dort auch meist Word- oder Exceldateien) von einem Webserver frisch ein tagesaktueller Virus nachgeladen.

Sollte der Virus aktiv werden können, so verschlüsselt er sämtliche Benutzerdaten (Dokumente, Bilder, Musik etc.), die er finden kann, sowohl lokal auf dem PC als auch auf allen verfügbaren Freigaben im Netzwerk. Die Verschlüsselung erfolgt per RSA nach AES-Standard der als sicher gilt (die gleiche Verschlüsselung nutzen i.d.R. Banken beim Onlinebanking). Daher hat man meist nur zwei Möglichkeiten an die Daten wieder heran zu kommen: Entweder über eine bestehende Datensicherung oder in dem man dem Erpresser das geforderte Geld zahlt (aktuell umgerechnet 200 – 1.000 Euro). Letzteres bietet natürlich noch keine Sicherheit, dass der Erpresser auch den Entschlüsselungscode liefert. In jedem Falls entsteht ein Ausfall Ihrer IT von einigen Stunden bis zu mehreren Tagen mit entsprechenden Kosten.

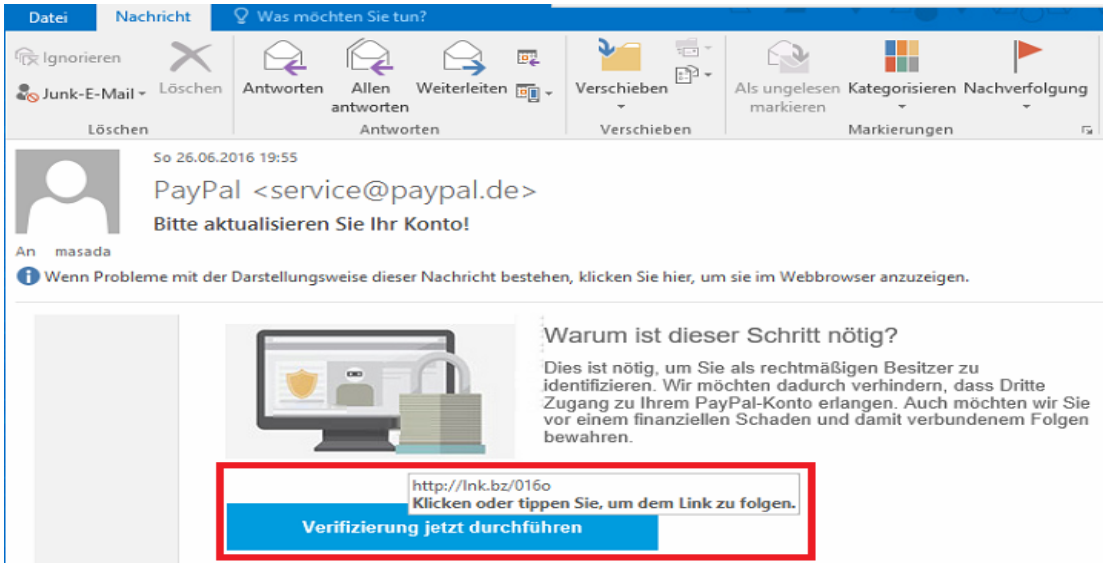
Daher ist es immens wichtig, sich zu schützen. Da bei dieser Art von Virus der Faktor Mensch eine entscheidende Rolle spielt, gibt es technisch keinen 100%igen Schutz. Es müssen alle Mitarbeiter sensibilisiert werden, um Fehleinschätzungen zu vermeiden.

## Vier wichtige Schritte bei E-Mails:

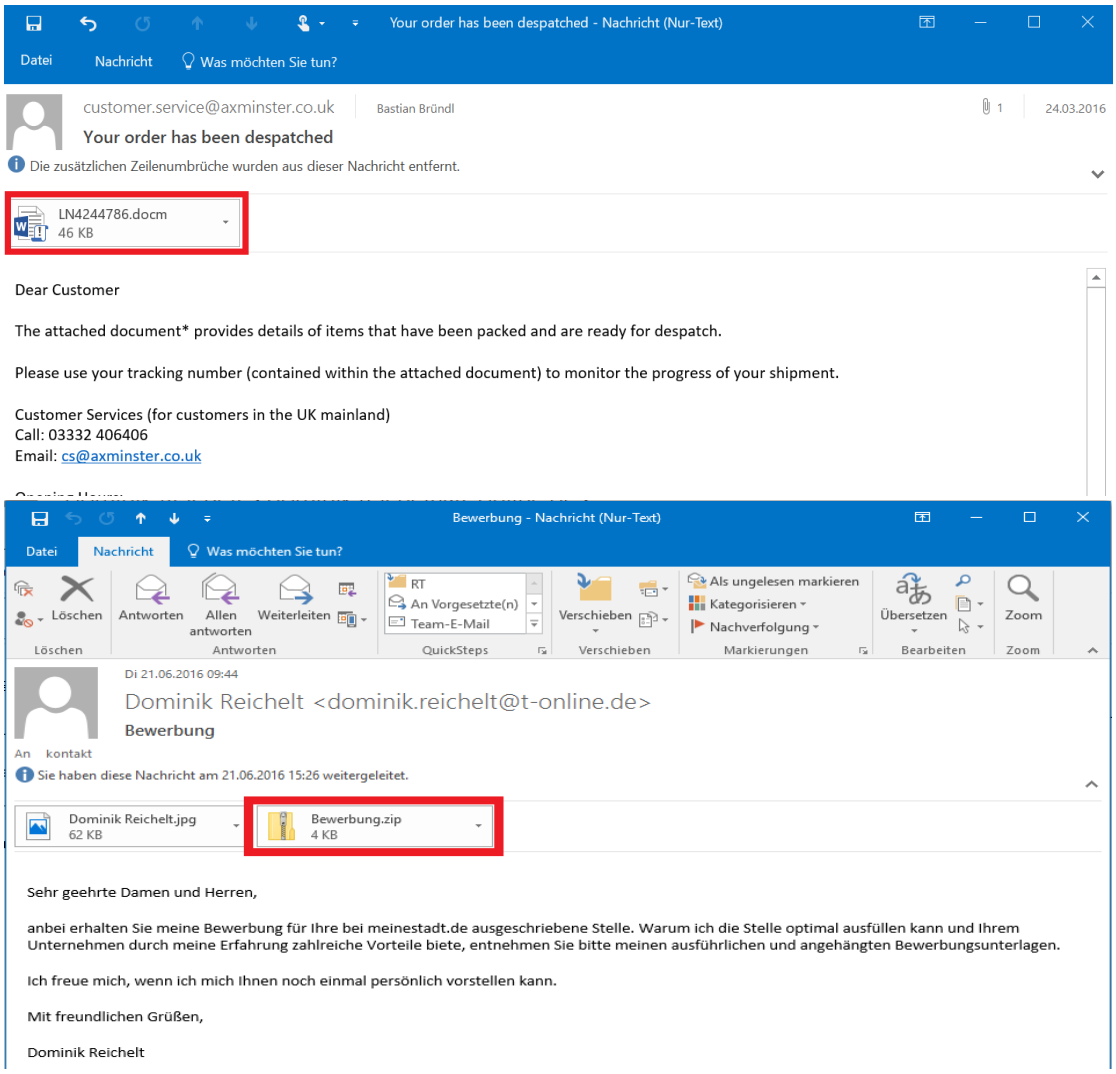
1. Absender überprüfen



2. Links überprüfen




3. Keine aktiven Anhänge (Microsoft Office: .doc/.docx/.xls/.xlsx/.ppt/.pptx) oder ZIP-Dateien unbekannter Absender öffnen (generell: Warum sollte man eine zip-Datei von 70kb Größe bekomm)




4. Wenn Sie sich nicht sicher sind: Rufen Sie uns an!