Security Awareness, Mail und Social Engineering

(Sensibilisierung der Mitarbeiter im Umgang mit Mails und deren manipulierenden Anweisungen)

SPD
Parteivorstand

10.07.17

Mail ist ein beliebtes Einfallstor für Angreifer, um Malware (=Schadsoftware) in Firmennetze einzuschleusen. Die heutige Technik erlaubt es dem Angreifer sein Opfer genau zu lokalisieren.

Der Angriff per Mail ist eigentlich eine Anwendung des sogenannten „Social Engineering“ - also sprichwörtlich die Manipulation von Menschen.

Die Sensibilisierung der Mitarbeiter ist daher ein wichtiger Punkt das Sicherheitsbewusstsein (Security Awareness) zu schärfen, um dieses Einfallstor zu verkleinern

Soziale Manipulation - Social Engineering

Die Manipulation von Menschen ist sehr einfach, weil Menschen weltweit ähnlich „verdrahtet“ sind und sich nur marginal durch kulturelle Gepflogenheiten unterscheiden. Die Grundmotivation aller Menschen ist gleich in Bezug auf ihren Nachwuchs, Existenzsicherheit und Befürchtungen.

Im Falle von Angriffen gibt es per Manipulation die Möglichkeit sich z.B. Zutritt zu Firmen zu verschaffen, dort auch in sensible Bereiche wie Rechnerräume.

Mail Angriffe

Ziel einer Mail mit manipulierenden Inhalt ist es, Schadsoftware auf dem Rechner zu installieren. Dies geschieht durch einen unbedachten Mausklick auf eine Web Seite oder auch durch Öffnen eines Dokuments.

Die Mail wird daher oft als Drohung oder als Anweisung, die zufällig mit der eigenen Situation zusammenpasst (erwartete Rechnung der Telekom etc.) inszeniert. Durch diese Manipulation wird meist in Panik oder ohne tiefere Kontrolle ein Link oder ein Anhang angeklickt. Die dann erreichte Webseite oder Anhang spielt innerhalb von Milli-Sekunden den Virus auf den Rechner. Dieser Virus wird auch personalisiert, d.h. er bekommt seine eigene Signatur und kann somit von den normalen Virenscannern nicht entdeckt werden.

Die aufgespielte Schadsoftware kann oftmals verschiedene Zielsetzungen haben: es gibt z.B. Keylogger, die alle Tastatureingaben an den Angreifer übermitteln, um Benutzerkonten und Passwörter abzugreifen.

Ebenfalls gibt es Software, welche den Rechner als Teil eines sog. Botnets konfiguriert, um seine Rechenleistung durch Dritte nutzbar zu machen.

Oder aber es werden die gesamten Daten der Festplatte verschlüsselt und der Benutzer soll Geld zahlen, um die Daten wieder zu entschlüsseln. In diesem Fall spricht man von Ransomware. Bekannte Fälle gingen auch durch die Presse, wie z.B. der Locky-Virus, WannaCry oder Golden Eye.

Wie kann man Angriffs-Mails erkennen?

Die erste Regel ist generell: beim Lesen einer Mail auf keinen Fall überhastet einen Anhang oder Link anklicken oder öffnen.

Viele Angriffsmails zeichnen sich aus durch grammatikalisch schlechtes Deutsch, Tippfehler oder eine fehlerhafte Mischung von Groß- und Klein-Schreibung.

Die Absenderadressen sind oft auch validen Firmen nachempfunden: z.B. wird anstelle von yahoo.com dann yahoo-inc.com verwendet.

Sehr vorsichtig sollte man sein, wenn der Name im Absender wie z.B. Eduard.Zimmermann@zdf.de unterschiedlich zur Signatur ist, z.B. Afred Biolek. Ja, in der Tat sind Angreifer so dumm und deswegen lohnt es sich immer genau zu gucken.

Plausibilität

Falls einem eine Mail verdächtig vorkommt, es aber eine gewisse Wahrscheinlichkeit gibt, dass sie legitim ist, weil sie ggf. von einem bekannten und validen Absender kommt, aber eigentlich „unerwartet“ ist vom Inhalt oder Timing her, lohnt es sich ein wenig Zeit zu investieren, die Mail gründlicher zu prüfen:

- Ist der Absender korrekt und/oder die Zeit? Schickt unser Anwalt wirklich um 3:53 früh eine Mail los?

- Schicken unsere Kunden uns eine Rechnung oder Mahnung? Eigentlich stellen wir unseren Kunden Rechnungen, die kaufen ja von uns?

- Bin ich überhaupt Mitglied bei Yahoo, PayPal oder der Stadtsparkasse, die mir gerade Mail geschickt hat? Bitte NICHT „forschen“, „warum die so blöd sind und auf mich kommen“ (O-Ton Opfer).

- Kann es wirklich sein, dass der Hausmeister einer entfernten Zweigstelle in mich verliebt ist? Ich habe den noch nie gesehen, noch nie telefoniert...

- Es lohnt sich ebenfalls die Datei-Endung genau anzusehen:
  .exe ist ein ausführbares Programm, sollte man wohl besser nicht ausführen
  .zip ist ein komprimiertes Archiv, oftmals enthalten diese Archive geschachtelte Archive, bis man schlussendlich wieder bei einer .exe Datei landet (Windows packt eine solche „ZIP-Bombe“ oft automatisch aus, ohne dass man es merkt).

Wie verfahren wir also weiter...?

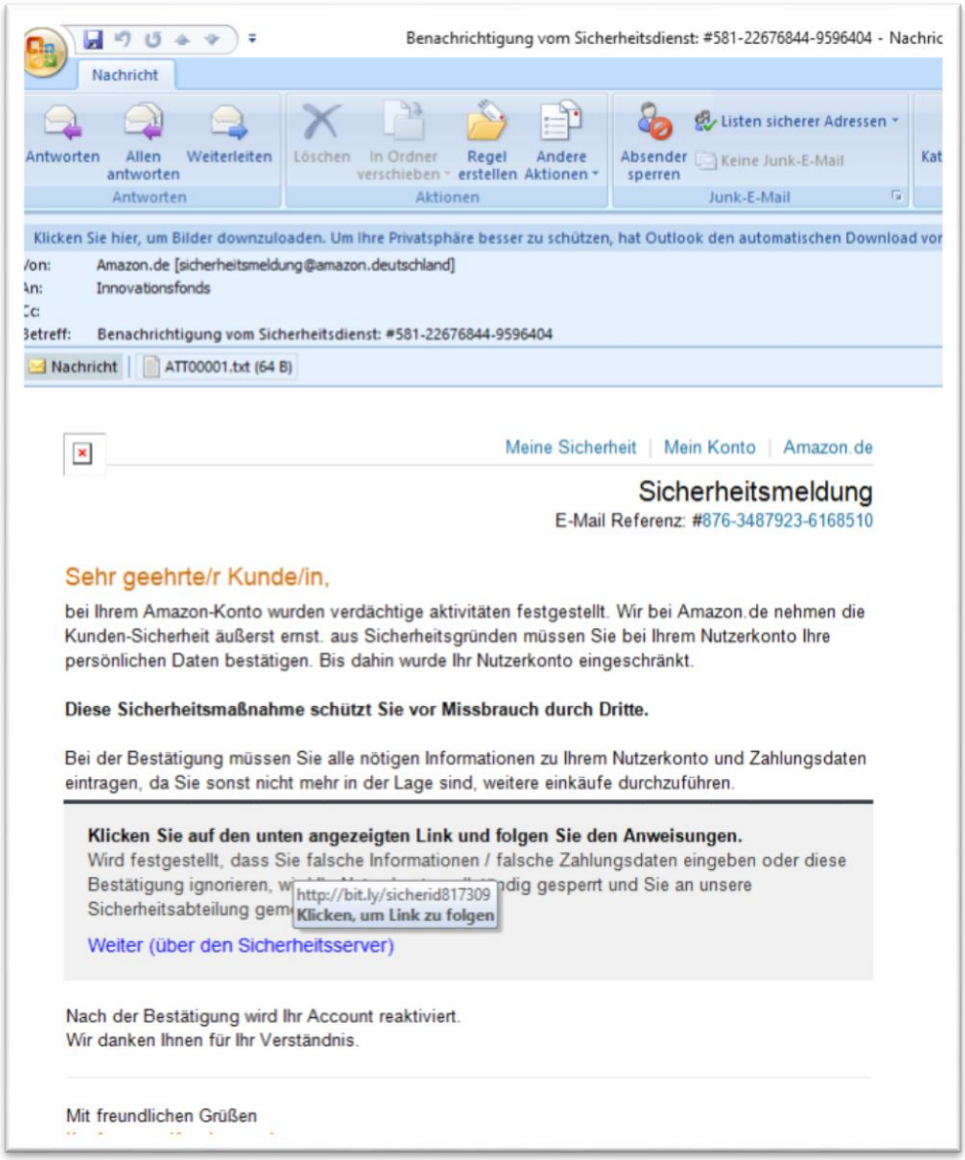
Verhaltensregeln für verdächtige Mails

Eigentlich gibt es für „offensichtlich“ gefälschte Spam Mails nur einen Weg: SOFORTIGE Löschung OHNE den Anhang zu öffnen oder ein enthaltenes Link zu klicken.

Links in Emails niemals anklicken. Es ist besser selbst diese Seiten im Browser einzugeben und zu der angegebenen Stelle zu surfen. So verhinderst du bei gefälschten Emails auf umgeleiteten Seiten zu gelangen.

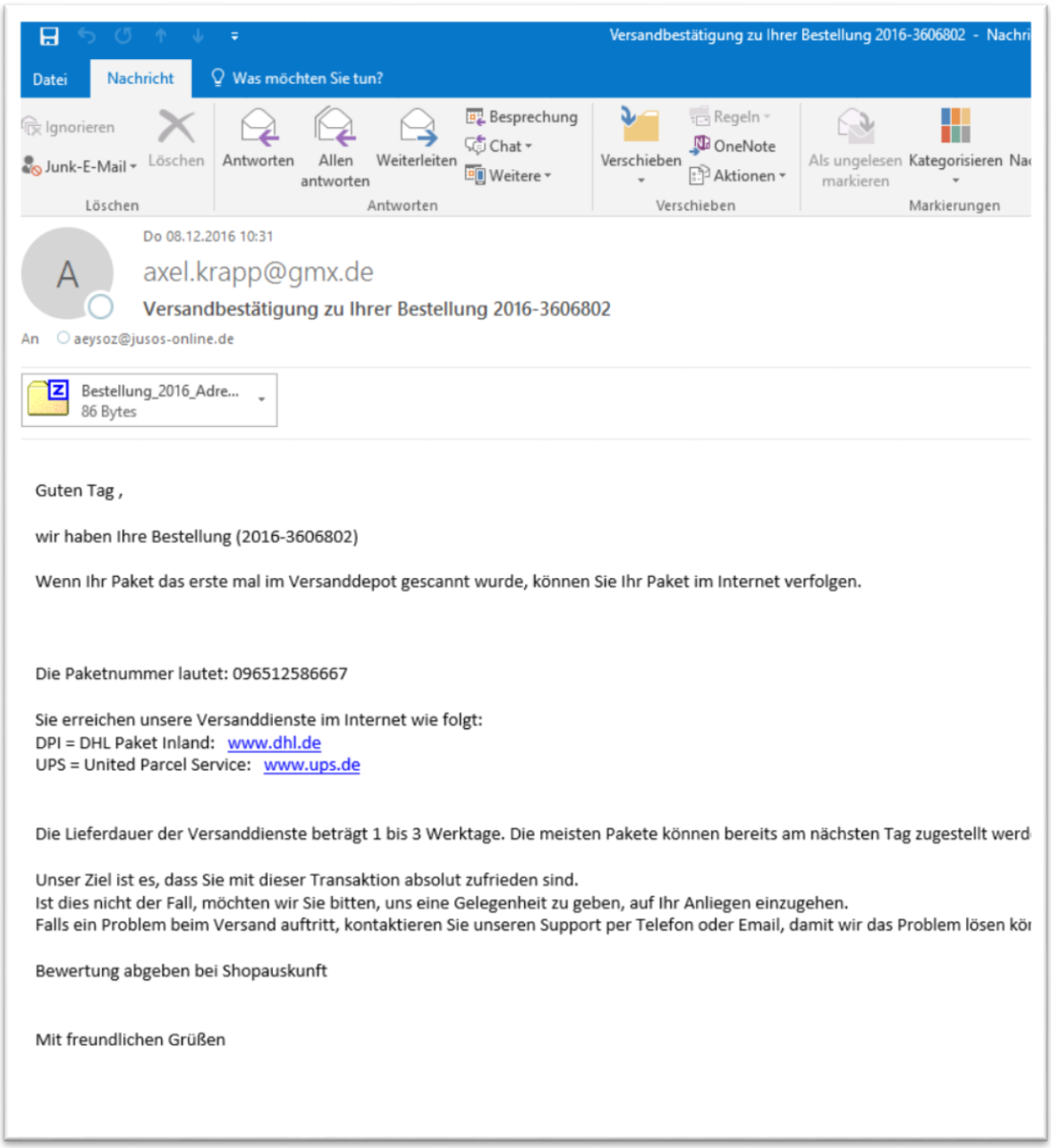
Beispiele:

Diese Email versucht einen Nutzer auf sein Amazon-Konto zu leiten. Schaut man sich den Link von „Weiter (über den Sicherheitsserver)“ an, dazu in Outlook mit dem Mauszeiger nur über den Link gehen, dann sieht man, dass der Link auf **keine** offizielle Amazon-Website zeigt.



Ist man sich doch unsicher. Klickt man **niemals** auf den Link, sondern geht selbst im Browser auf Amazon.de und meldet sich an seinem Konto an, um diese Informationen zu prüfen.

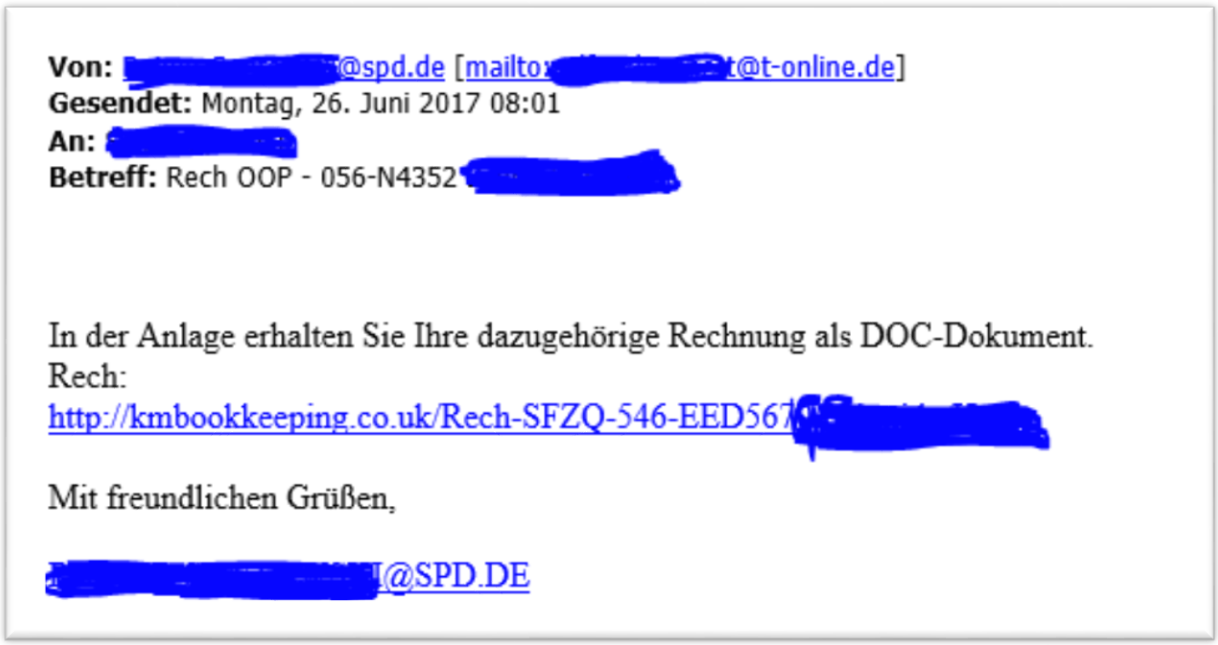
Im nächsten Beispiel versucht der Absender mit einer nicht genauer spezifizierten Versandbestätigung den Nutzer dazu zu bewegen sich die fehlenden Informationen über die angehängte ZIP-Datei zu besorgen. Sollte einem der Absender nicht bekannt sein, dann löschen.



Ist der Absender bekannt, aber die Bestellung nicht, trotzdem **nicht** auf die ZIP-Datei klicken. Hier hilft nur die telefonische Rückfrage oder Rückfrage über eine neue Email (nicht auf Antworten klicken). Bei der telefonischen Rückfrage, verwendet **nur** euch bekannte Rufnummern. In Emails angegebene Rufnummern können auch gefälscht sein.

In einem weiteren Beispiel kennt der Empfänger den Absender, der angezeigte Emailname …@spd.de ist auch bekannt nur die „mailto:“ -Adresse mit @t-online.de war unbekannt.

Weiterhin ist im Link der eigene Name angegeben. Er enthält zwar ein Dokument, welches aber einen Virus/Trojaner auf den Computer lädt.



Von: [redacted]@spd.de [mailto:[redacted]t@t-online.de]
Gesendet: Montag, 26. Juni 2017 08:01
An: [redacted]
Betreff: Rech OOP - 056-N4352[redacted]

In der Anlage erhalten Sie Ihre dazugehörige Rechnung als DOC-Dokument.
Rech:
http://kmbookkeeping.co.uk/Rech-SFZQ-546-EED567[redacted]

Mit freundlichen Grüßen,

[redacted]@SPD.DE