Schadmails sicher erkennen

90% aller Schadsoftware wird in Firmennetzwerke dadurch eingeschleust, dass unreflektiert und voreilig Mailanhänge geöffnet werden oder auf Links in Mails geklickt wird. Viel Schadsoftware wird zwar durch vorgeschaltete Programme (Mailfilter etc.) abgefangen, aber nicht alle. Gerade die pfiffig gemachten Mails kommen durch. Hier hilft nur, auch in der Alltagshektik, genau zu schauen!

Typische Indizien, dass es sich um eine Schadmail handelt, sind die folgenden:

- In der Mail finden sich Rechtschreibfehler.
- In der Mail finden sich Reste von HTML-Befehlen wie `<b>`, `</b>` oder auch `<p>`.
- Die Mail ist in fremder Sprache.
- Es sind logische Brüche in der Mail, bspw. kommt eine Edeka-Mail von einer Domain `kundenbetreuung@hornbach.com`.
- Die deutschen Umlaute werden nicht richtig dargestellt, bspw. das ä als ÃÃ¼.
- Es gibt keine persönliche Adressierung, stattdessen wird eine Mail-Adresse als Anrede gewählt, bspw. „Sehr geehrter max.mustermann@t-online.de“
- Es geht um Sex oder Potenz.
- Man wird aufgefordert, höchstpersönliche Daten einzugeben, bspw. Kontonummer, Geburtsdatum, Ausweisnummer, PIN-Kode etc.
- Man wird angeschrieben von einer völlig unbekannten Person.
- Die Mail-Adresse stimmt nur fast, bspw. `noreply@amzon.com` anstelle von `noreply@amazon.com`
- Man wird angeschrieben von einer Person des öffentlichen Lebens, bspw. Günter Jauch, der den Kauf von BitCoins empfiehlt.
- Die Mail stammt von einer kryptischen Mail-Adresse, bspw. `66gdi86t54eh76529@atl86327tx.com`
- Es wird das Blaue vom Himmel versprochen, bspw. werden wahnsinnige Rabatte versprochen.
- Es werden Bedürfnisse geweckt, bspw. „Schau mal, wo ich dich verlinkt habe“.
- Es wird zeitlicher Druck aufgebaut, es muss sofort oder innerhalb einer kurzen Friste entschieden (= geklickt) werden.
- Es wird emotionaler Druck aufgebaut, bspw. dass man beim Onanieren gefilmt wurde.
- Im Anhang findet sich eine Datei, die auf EXE, ZIP, BAT o.ä. endet.

<u>Keine</u> sicheren Zeichen für eine unbedenkliche Mail sind folgende:

Die Mail stammt von einer persönlich bekannten Mail-Adresse	Wer als Absender einer Mail erscheint, kann vom Sender frei gewählt werden. Erst aus dem Mail-Header kann man erkennen, welchen Weg die Mail genommen hat. Der aber wird in Programmen wie Outlook nicht angezeigt.
In der Mail werden höchstpersönliche Daten genannt, bspw. „Sie als Bürokraft …“	Schadmails werden millionenfach verschickt. Darunter werden dann schon ein paar tausend Bürokräfte sein, die sich angesprochen fühlen.
In der Mail werden höchstpersönliche technische Daten genannt, bspw. „Ihre gegenwärtige IP-Adresse lautet …“	Diese Daten kennt der Schreiber tatsächlich nicht. Sie werden vom eigenen Computer generiert und eingefügt.
Die Mail sieht täuschend echt aus, ganz so, wie die vom echten Unternehmen.	Echte Mails werden einfach nur kopiert, schließlich verschickt das echte Unternehmen ja alle Texte, Schriftarten, Graphiken etc. immer mit seinen Mails mit.
Ein Anhang ist auf den ersten Blick eine Word-Datei, sie heißt `Antrag.doc.bat`	Maßgeblich ist immer nur das letzte Suffix, hier als BAT. Alles was davor steht, ist egal. Tatsächlich ist es eine ausführbare Datei.

Stand 3/2022