Sicherer Umgang mit E-Mails

Obwohl alle ein- und ausgehende E-Mails mehrfach von Viren Scannern und Firewalls geprüft werden gibt es leider keinen 100%igen Schutz.

Man sollte nie davon ausgehen, dass alle eingehenden E-Mails „sauber“ und ungefährlich sind. Es kann immer wieder vorkommen, dass E-Mails gefährliche Inhalte enthalten.

Eine erhöhte Aufmerksamkeit und ein gesundes Maß an Misstrauen kann die Sicherheit erhöhen.

Folgende Verhaltensempfehlungen für den betrieblichen, aber auch den privaten Umgang mit E-Mails sollten verinnerlicht werden.

Eine allgemeingültige Aussage, wie Viren in E-Mails erkannt werden, gibt es nicht.

Es gibt allerdings einige Regeln, die befolgt werden sollten:

Vorsicht bei jedem Attachement
Computerviren stecken in der Regel fast nie direkt in der E-Mail, sondern in den angehängten Dateien. Daher sollte genau überlegt werden, ob ein Anhang geöffnet wird oder nicht.

Sinnhaftigkeit hinterfragen
Beispiele:

- Englischer Text oder Betreff von einer deutschen bekannten E-Mail
- Rechnungen von einer Kunden-E-Mail
- Rechnungen, Buchungsbestätigungen, etc. generell Inhalte die so nicht zum Tagesgeschäft gehören
- Wichtige Schreiben von Anwälten oder Banken werden nicht per E-Mail versendet
- Es werden falsche oder keine Anreden verwendet
- Rechtschreibfehler im Text

Absender jeder E-Mail misstrauen
Der Absender einer E-Mail lässt sich mit den einfachsten Mitteln fälschen. Im Zweifelsfall sollte telefonisch beim Absender nachgefragt werden.

Nicht gebucht, ist nicht gebucht
Eine beliebte Methode, um zum Öffnen eines Anhangs zu verführen, sind gefälschte Buchungsbestätigungen oder Rechnungen von scheinbar großen, bekannten Anbietern wie 1&1, Hotel.de, DHL, Telekom, O2, vodafone, Amazon, PayPal etc. zu verschicken. In der E-Mail wird dann eine nie getätigte Buchung oder Bestellung bestätigt oder Rechnung versendet und aufgefordert, den Anhang zu öffnen. Es handelt sich dabei um einen Virus!

Es gibt keine Sicherheitsupdates per E-Mail!
Eine E-Mail, welche auffordert, mit einem Link oder einem Anhang ein Sicherheitsupdate z.B. für Windows oder eine Banking-Software durchzuführen, ist ebenfalls gefährlich. Diese E-Mail muss sofort gelöscht werden. Es gibt keine Sicherheitsupdates per E-Mail.

Dateien mit folgenden Endungen nie öffnen
.exe .bat .com .vbs .pif - auch nicht, wenn der Absender der E-Mail bekannt ist. Dateien dieses Typs enthalten ausführbare Programme, welche die Computer befallen. Auch bei anderen Endungen ist Vorsicht geboten.
Die genannten sind allerdings besonders gefährlich und sollten immer ignoriert werden. Dies gilt besonders für "Mogelendungen", z.B. protocol.doc.exe scheint auf den ersten flüchtigen Blick eine Word-Datei zu sein, aber in Wirklichkeit hat sich mit der Endung .exe ein Virus eingeschlichen.

Kühlen Kopf bewahren
Eine weitere Möglichkeit, den Nutzer zum Öffnen eines E-Mail-Anhangs zu verführen, in dem sich das Virus verbirgt, ist die Erzeugung psychischen Drucks und Nervosität.
Anbei ein paar Beispiele:

- Es wurde ein Strafverfahren gegen Sie eröffnet, bitte beachten Sie umgehend die Anhänge dieser E-Mail!
- Ihre Kreditkarte wurde missbräuchlich benutzt. Weitere Details im Anhang dieser E-Mail!
- Ihr Amazon-Konto wurde geknackt. Weitere Details finden Sie im Attachement dieser E-Mail.
- Auf Ihrem Computer wurde ein Virus entdeckt. Im Anhang dieser E-Mail finden Sie Informationen, wie der Virus entfernt werden kann.

Es sollte davon ausgegangen werden, dass solche E-Mails immer gefälscht sind. Bei Unklarheit sollte im Internet genauer recherchiert werden. Auf solche E-Mails sollte nie geantwortet werden oder die darin enthaltene Rufnummer kontaktiert werden.

Weiter sollten verdächtige E-Mails nie weitergeleitet werden, besser wäre es hier einen Screenshot der E-Mail zu erstellen oder in einer separaten E-Mail dem Vorgesetzen den Sachverhalt zu schildern.