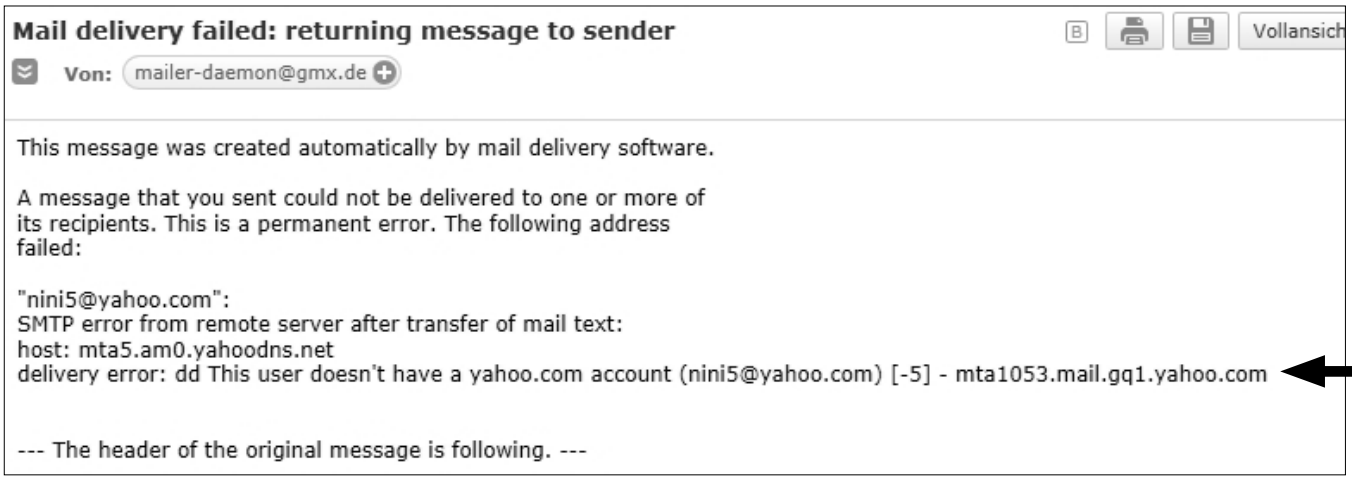
Warnung vor gefälschten Emails! (2)

Gernot L. Geise



Die Meldung des „Mailer Daemons". Aus der vorletzten Zeile (Pfeil) geht hervor, dass es diese Adresse nicht gibt (Den unteren Teil dieser Email habe ich weggelassen, er zeigt nur in kryptischen Zahlen- und Buchstabenkombinationen den Weg durchs Netz).

Es geht weiter

Seit einigen Wochen kursieren Emails, die so aussehen, als ob sie von unserem Mitglied Nicole Albert stammen würden. Als Inhalt ist kommentarlos nur ein Link angegeben.

Ein Empfänger, der Nicole kennt, denkt sich nichts Böses dabei, da sie in unregelmäßigen Abständen Info-Emails versendet. Das Erwachen kommt erst, wenn man den Link anklickt und dann auf recht ominöse Seiten geleitet wird, etwa Glücksspielseiten und Schlimmeres.

Wer achtet schon darauf, wenn bei einer (eigentlich bekannten) Email-Adresse „com" anstatt „de" angehängt ist? Die korrekte Email-Adresse von Nicole lautet nämlich nini5@yahoo.**de**. Und die Spam-Email hat die Adresse nini5@yahoo.**com**!

Ich klickte zunächst auf den „Beantworten"-Knopf, um bei Nicole anzufragen, was diese Email soll. Doch jetzt stellte sich heraus, dass es diese Email-Adresse nicht gibt! Denn wenn man eine Email an eine nicht existierende Adresse schickt (das kann auch eine falsch geschriebene sein, etwa durch Buchstabendreher), dann meldet sich der „Mailer Daemon". Das ist ein Programm, mit dem der Email-Verkehr überwacht wird. Öffnet man eine „Mailer Daemon"-Email, so werden dort auf englisch u. a. der Absender, Empfänger und gesamte Laufweg angegeben, sowie kryptisch verschlüsselt der Email-Inhalt. Im genannten Fall geht dann daraus hervor, dass es die Empfänger-Adresse nicht gibt (siehe Abb.).

Inzwischen kursieren auch Emails mit anderen Adressen, offensichtlich vom selben Hacker erstellt. Auch in ihnen ist kommentarlos nur ein Link angegeben.

Wer solche Emails zusammenbastelt, wer unter falschen oder erfundenen Email-Adressen Spams versendet, lässt sich leider nicht ermitteln.

„Normale" Spam-Emails sehen etwa so aus: Im Betreff „Bestellbestätigung". Da sagt man sich unwillkürlich, was das soll, weil man nichts bestellt hat, und öffnet die Email. Darin steht dann: *„Ich habe versucht dich anzurufen, jedoch ohne Erfolg."* Kann ja nicht sein, sonst wäre der Anruf auf dem Anrufbeantworter, sagt man sich. Weiter in der Email geht es dann darum, dass man eine Software installieren soll, um damit an der Börse „garantierte Verdienste" zu machen. Nachtigall, ick hör dir trappsen!

Es gibt nur eine Möglichkeit, lästige Emails loszuwerden, die nicht automatisch im Spam-Ordner landen: Mysteriöse Emails von unbekannten Absendern kommentarlos löschen, denn man weiß nicht, was man sich bereits mit dem Öffnen einer solchen Email für Schadprogramme auf den Rechner lädt! Die „Hacker"-Szene ist sehr erfinderisch!

Es ist auch sinnvoll, bei unbekannten Emails zunächst den Absender näher zu betrachten. Oftmals kann man anhand des globalen Teils erkennen, woher die Email stammt.

Emails bestehen aus dem „lokalen" und dem „globalen" Teil, die durch das „@"-Zeichen voneinander getrennt sind. Der lokale Teil ist der Inhabername einer Email, wobei auch sinnlose Namen, Zahlen, „info" o. ä. zur Anwendung kommen können. Der globale Teil enthält den Namen des Providers, durch den man ins Netz geht, z. B. „t-online.de" oder auch etwa „efodon.de". Die Buchstabenkombination hinter dem Punkt steht entweder für ein Landeskürzel (etwa „.de", „.eu") oder „.com", „.gov", „.net", aber auch „.info", „.tv" usw. Wobei das beliebte Kürzel „.tv" ein Landeskürzel für eine recht unbekannte Insel ist, die sich „.tv" rechtzeitig reservieren konnte und seither durch seine Verwendung ordentlich verdient. ■