Sicherheits-Quickie

Gefälschte E-Mails im Namen von Freunden, Nachbarn und Kollegen gefährden ganze Netzwerke. Die Bedrohung durch Schadsoftware nimmt weltweit täglich zu und verursacht auch in Deutschland aktuell hohe Schäden.
Oft wird Schadsoftware über Spamkampagnen verteilt. Besonders Auffällig ist hier aktuell die Schadsoftware Emotet. Sie nistet sich unbemerkt in Ihrem System ein und liest Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern der infizierten Systeme aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung der Schadsoftware, indem sie den Empfängern identisch aussehende E-Mails, allerdings mit erfundenen Inhalten von Absendern schicken mit denen die Empfänger erst kürzlich in Kontakt waren. Auf Grund der authentischen Erscheinung der Nachrichten, verleiten sie den Empfänger zum unbedachten Öffnen der schädlichen Dateianhänge oder der in der Nachricht enthaltenen URL.
Ist die Software einmal auf dem Rechner, lädt sie weitere Schadsoftware nach, wie z.B. den Banking-Trojaner Trickbot. Diese Schadprogramme führen zu Datenabfluss und ermöglichen den Tätern ggf. sogar die Kontrolle über das gesamte System.
Ein paar einfache Grundregeln zu beachten hilft oft schon, den Ernstfall gar nicht erst eintreten zu lassen. Ohne zusätzliche Kosten! (Wenn Sie bereits AV-Software einsetzen)

Wie Sie sich schützen können:

- Installieren Sie zeitnah bereitgestellte Sicherheitsupdates für Betriebssysteme und Anwendungsprogramme (Web-Browser, E-Mail-Clients, Office-Anwendungen usw.).
- Setzen Sie Antiviren-Software ein und aktualisieren Sie diese immer wieder.
- Sichern Sie regelmäßig Ihre Daten (Backups).
- Richten Sie ein gesondertes Benutzerkonto auf dem Computer ein, um zu surfen und E-Mails zu schreiben.
- Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge von E-Mails (insbesondere Office-Dokumente) und prüfen Sie in den Nachrichten enthaltene Links, bevor sie diese anklicken. Bei einer verdächtigen E-Mail sollten Sie im Zweifelsfall den Absender anrufen und sich nach der Glaubhaftigkeit des Inhaltes erkundigen.

Was Sie tun können, wenn Sie betroffen sind:

- Informieren Sie Ihr Umfeld über die Infektion, denn Ihre Mailkontakte sind in diesem Fall besonders gefährdet.
- Ändern Sie alle auf dem betroffenen System (zum Beispiel im Web-Browser) gespeicherten und eingegebenen Zugangsdaten.
- Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten System vor. Sollte Ihr Rechner mit Schadsoftware infiziert sein, dann sollten Sie diesen Rechner neu aufzusetzen.