# Angriffe auf die Datensicherheit II: Trojaner, Hoaxes

## Trojaner

Der Trojaner oder das Trojanische Pferd hat seinen Namen aus der griechischen Mythologie: Nachdem die schöne Helena entführt worden war, belagerten die Griechen Troja, um sie zu befreien. Trotz zehnjähriger Belagerung gelang dies aber nicht. Odysseus hatte schließlich die Idee, ein hölzernes Pferd zu bauen, in dem sich einige Soldaten versteckten. Die übrige griechische Armee zog sich zurück. Die Trojaner dachten, die Griechen hätten die Belagerung aufgegeben, und hielten das Pferd für ein Geschenk. Sie zogen das Pferd in die Stadt. In der Nacht stiegen die Soldaten aus dem Pferd und öffneten der übrigen Armee die Tore. So war Troja besiegt.

Trojaner funktionieren nach einem ähnlichen Prinzip. Es sind eigenständige Programme, die oftmals (aber nicht immer) eine für den Anwender recht nützliche oder interessante Funktion haben. Im Verborgenen tun sie aber eigentlich etwas anderes. Die Schadfunktion läuft dabei für den Anwender völlig unsichtbar im Hintergrund ab. Manche Trojaner tarnen sich als Spiele oder nützliche Tools, die zum Beispiel über einen E-Mail-Wurm oder als Download aus dem Internet weiterverbreitet werden, manchmal wird die angeblich nützliche Funktion auch nur behauptet (wenn man das vermeintlich tolle Tool dann anklickt, geschieht nichts Offensichtliches, aber im Hintergrund installiert sich der Trojaner).

Was tun Trojaner? Trojaner sind mit Abstand die gefährlichste Art von Schadprogrammen, die in diesem Abschnitt behandelt wurden. Sie spähen zum Beispiel Kennwörter, Konto- und Kreditkartendaten aus und versenden sie an Betrüger. Manche Trojaner können auch verwendet werden, um weitere Software auf einem Computer zu installieren. Läuft also erst einmal solche ein Trojaner auf einem Rechner, kann er verwendet werden, um nahezu jede andere Funktionalität in den Computer einzuschmuggeln. Mithilfe mancher Trojaner kann der Rechner regelrecht ferngesteuert werden. In der Tat können einige Trojaner auch als Verwaltungsprogramme verwendet werden, um zum Beispiel bestimmte Funktionen remote auf einem Rechner ausführen zu können. Geschieht dies aber ohne Wissen des eigentlichen Besitzers, sind diese Tools eine gefährliche Waffe[1].

Häufig werden Computer zum Beispiel missbraucht, um Werbe-E-Mails zu versenden oder andere Rechner anzugreifen. Die Möglichkeiten sind fast unbegrenzt.

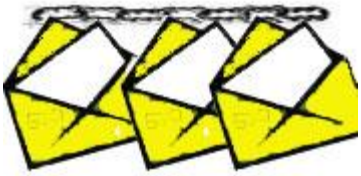
Entsprechend hoch ist der Schaden, der durch Trojaner angerichtet wird.

---

[1] Ein bekanntes Beispiel eines solchen Fernwartungstrojaners ist Back Orifice bzw. Back Orifice 2000. Diese Software ermöglicht es dem Angreifer u. a. Dateien zu lesen, zu schreiben, zu löschen und herunterzuladen und mit einem zusätzlichen Plug-In den Bildschirm anzuzeigen und sogar die Kontrolle über Maus und Tastatur zu übernehmen. Außerdem können Programme gestartet, Kennwörter ausgelesen, Verzeichnisse erstellt werden und vieles mehr.

Abbildung: http://www.borg-krems.ac.at/mediawiki/index.php/Bild:Trojaner1.jpg, 05.12.09

## Hoaxes und Kettenbriefe



Hoaxes werden hier nur als Randphänomen betrachtet. Der Begriff Hoax bedeutet auf Deutsch so viel wie „Falschmeldung“ oder „(Zeitungs-)Ente“. Hoaxes sind Kettenbriefe, die als E-Mail versendet werden und deren Hauptziel es ist, den Empfänger dazu zu bringen, die Mail weiterzuleiten. Dabei enthalten sie oft die (falsche) Warnung vor einem sehr gefährlichen neuen Virus/Wurm/Trojaner. Kettenbriefe verfolgen dasselbe Ziel der Weiterverbreitung wie Hoaxes, haben aber eher einen nichttechnischen Inhalt. Sie drücken zum Beispiel auf die „Tränendrüse“, indem sie Geschichten von Menschen mit angeblich schweren Schicksalen benutzen, sie prophezeien Glücks- oder Unglücksfälle, wenn die Mail nicht weitergeleitet wird, oder sind Teil eines Schneeballsystems, das traumhafte Gewinne verspricht.

Was haben Hoaxes und Kettenbriefe nun im Abschnitt Datensicherheit zu suchen? Worin besteht die Gefahr?

In erster Linie sind Hoaxes und Kettenbriefe ein Ärgernis, denn sie „fressen“ Computer- und Netzwerkressourcen und Arbeitszeit. Gefährlich sind Hoaxes aber zum Beispiel auch, wenn sie Anweisungen geben, wie man denn nun der angeblich drohenden Gefahr entfliehen könnte. Es gibt häufig Hoaxes, die dazu auffordern, vermeintliche Virendateien zu löschen. Benutzer, die diesen Anweisungen folgen, löschen unwissentlich wichtige Systemdateien, was im Zweifelsfall die Funktion des Systems komplett lahmlegen kann. Ein Beispiel dafür ist der Hoax W32.MFG.Tassos@mm (siehe http://www2.tu-berlin.de/www/software/hoax/tassostxt.shtml), der vor einem gleichnamigen Virus warnt. Benutzer, die der Anleitung zur angeblichen manuellen Entfernung des (nicht existierenden!) Virus folgen, löschen dabei die Verwaltungskonsolen von Windows und schließlich eine der Startdateien, sodass Windows anschließend nicht mehr startet.

Abbildung: http://www.polizei.bayern.de/kriminalitaet/internet/betrug/index.html/56984, 05.12.09