Bundesamt für Sicherheit in der Informationstechnik

Schadprogramme

Gefahren lauern überall – auch im Internet. Wer seine Daten nicht schützt, macht es Feinden einfach, diese bei der Übertragung mitzulesen, zu verändern oder sogar zu löschen. Man hört immer öfter von neuen **Viren** oder **Würmern – Programmen** also, die sich selbständig verbreiten oder über E-Mails versandt werden und Schäden auf Ihrem PC anrichten können. Aber auch von **Trojanischen Pferden** ist oft die Rede. Das sind dann Programme, die vom Nutzer unbemerkt sicherheitskritische Funktionen durchführen, indem sie beispielsweise Passwörter abfangen.

Schädliche Programme für den Computer werden heute nicht mehr vorrangig von Einzeltätern geschrieben, die sich damit in ihrer Clique beweisen wollen. Sie sind schon längst von kriminellen Netzwerken abgelöst worden, die international operieren, arbeitsteilig organisiert sind und es auf das Geld der Internetnutzer abgesehen haben.

Die Familie der IT-Schädlinge

Früher nannte man schädliche Programme aufgrund ihrer Eigenschaften meist "Viren". Heute sprechen Experten generell von "Schadprogrammen" und meinen damit alle bösartigen Programme, die auf von ihnen befallenen Rechnern unerwünschte Funktionen ausführen. Viele dieser Schädline sind heute modular aufgebaut und können darum häufig nicht eindeutig einer bestimmten Kategorie - etwa Virus oder Wurm - zugeordnet werden. Inzwischen sind diese Programme zudem so raffiniert, dass sie über das Internet automatisch weitere Funktionen nachladen und sich ständig verändern können.

Viele Exemplare haben eine weitere unangenehme Eigenschaft: Sie versuchen, andere Rechner im Internet ebenfalls zu infizieren. Zu diesem Zweck haben ihre Programmierer viele verschiedene Angriffsmethoden, die z.B. Schwachstellen in gängigen Internetbrowsern oder im Betriebssystem ausnutzen, in ihre Schadprogramme implementiert, die vollautomatisch eine nach der anderen ausprobiert werden. Dieses Vorgehen gleicht einem Einbrecher, der nacheinander Türen und Fenster auf Schwachstellen untersucht, um möglichst schnell und unauffällig ins Haus zu gelangen.

So kommen die Schädlinge auf Ihren Rechner

Ganz zu Beginn des PC-Zeitalters waren austauschbare Datenträger wie Disketten oder CD-ROMs die wichtigsten Verbreitungswege für Schadprogramme. Dann kam das Internet und mit ihm die globale Vernetzung von Computern. Das eröffnete den Tätern neue Kanäle zur Verbreitung von schädlicher Software. Zunächst wurden die Schädlinge bevorzugt per E-Mail versandt: Sie verstecken sich in einem Anhang, der dem Empfänger beispielsweise eine nützliche Information verspricht oder angeblich eine Rechnung enthält. Wer diese Datei anklickt, holt sich den Schädling auf seinen Rechner.

Seit einiger Zeit verfolgen die IT-Kriminellen zusätzlich eine neue Strategie: Sie infizieren Webseiten mit schädlichem Code. Es kann vorkommen, dass seriöse populäre Webseiten von Cyber-Kriminellen gecrackt und mit Schadcode versehen werden, beispielsweise über einen eingeblendeten Werbebanner, der von einem anderen Server geladen wird. Wenn Ihr Rechner Schwachstellen hat, reicht es also aus, eine solche Internetseite zu besuchen, um sich einen Schädling einzufangen. Weil der Nutzer davon nichts bemerkt und auch gar nichts weiter dazu beitragen muss - etwa auf eine Datei klicken -, nennt man diesen Infektionsweg Drive-by-Download (also im "Vorbeifahren").

Das darf jedoch nicht darüber hinwegtäuschen, dass die klassischen Verbreitungsmethoden nach wie vor Verwendung finden. Beispielsweise verbreitete sich der bekannte Conficker-Wurm auch über USB-Sticks.

Auch bei Datei-Downloads aus dem Internet ist Vorsicht geboten: In der Flut von Dateien und Gratis-Programmen im Internet verstecken sich zahlreiche Schädlinge. Besonders Raubkopien und Programme für illegale Zwecke (etwa zum unerlaubten "Knacken" kostenpflichtiger Programme) sind häufig mit bösartigen Funktionen verseucht.