

# Schadprogramme

## Arten von Schadsoftware

### *Backdoor*

Eine Backdoor (auf Deutsch: Hintertür) ist ein Schadprogramm, das Sicherheitsmaßnahmen umgeht, um dann die Kontrolle über einen Computer zu erlangen. Auf diese Weise kann der Angreifer persönliche Daten ausspionieren oder weitere Schadprogramme installieren.

### *Bootvieren*

Sie verändern den Startbereich von Disketten und Festplatten. Das Kann z.B. den Start des Betriebssystems verhindern.

### *Dialer*

Sogenannte Dialer (auf Deutsch: Einwahlprogramme) können selbstständig eine Telefonverbindung aufbauen und damit extrem hohe Kosten verursachen. Sie funktionieren allerdings nur, wenn Sie per Modem oder ISDN ins Internet gehen und nicht über DSL.

### *Hoax*

Ein Hoax (auf Deutsch: Schabernack) heißt eine Falschmeldung, die meist per E-Mail verbreitet wird. Oft wird über Virenfalschmeldungen versucht Angst zu schüren oder Benutzer zu sinnlosen Aktionen zu verleiten. Etwa: „Löschen Sie die Datei XY, um Ihren PC zu schützen.“

### *Keylogger*

Keylogger (auf Deutsch: Tasten-Rekorder): Er kann alle Tastatureingaben des Nutzers aufzeichnen und über das Internet an einen Angreifer schicken. So spionieren Gauner geheime persönliche Daten aus, etwa Passwörter oder PINs fürs Online-Banking.

### *Makrovieren*

Ein Makro ist ein Programm, das in einem Dokument eingebaut ist und kleine nützliche Aufgaben erfüllt. So kann ein Makro automatisch Adressen in einen Serienbrief einfügen. Enthält ein Makro einen Virus, kann der sich auf andere Dokumente übertragen und Daten verändern oder löschen.

### *Polymorphe Viren*

Sie verändern selbstständig ihren eigenen Quellcode. Auf diese Weise sollen sie ihre Erkennung durch Schutzprogramme verhindern.

### *Rootkit*

Sie können sich und andere Schädlinge vor Virenschutz-Programmen verstecken. Einmal aufgespielt, greifen Datenräuber unbemerkt auf den Computer zu.

### *Wurm*

Ein Wurm verbreitet sich selbstständig über Computernetzwerke, etwa durch E-Mails. Er richtet nicht unbedingt direkt Schaden an. Da er sowohl auf den infizierten Computern als auch in den Netzwerken für jede Menge Wirbel sorgt, kann er allerdings hohe Kosten verursachen. Etwa indem er den Datenverkehr blockiert oder andere Schadprogramme aus dem Internet nachlädt.

### *Spyware/Adware*

Das sind Programme, die sich oft in kostenloser Software verstecken. Spyware sendet persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte, etwa welche Seiten Sie im Internet besuchen. Adware blendet unerwünschte Werbung ein.

### Trojaner

Diese Programme gaukeln vor, eine bestimmte Funktion zu haben. In Wahrheit erledigen sie aber ganz andere Aufgaben. Einige Trojaner laden andere Schadprogramme nach oder spionieren persönliche Daten aus. Sie vermehren sich nicht selbst, was sie von Viren und Würmern unterscheidet.

### Prävention

- Aktuelles Viren-Schutzprogramm
- Firewall aktivieren
- Sicherheitsupdates des Betriebssystems
- Möglichst kein Administrator account verwenden
- Browser mit integrierter Funktion zur Erkennung von böartigen Webseiten verwenden
- Passwörter in regelmäßigen Abständen wechseln
- Vorsicht mit E-Mail-Anhängen
- Vorsicht bei Downloads von Webseiten (vergewissern Sie sich auf die Vertrauenswürdigkeit)
- Zurückhaltend mit der Weitergabe von persönlicher Information
- Bei Voice oder IP (VoIP) oder WLAN auf Verschlüsselung achten
- Regelmäßige Sicherungskopien der Daten auf externen Festplatten/Clouds erstellen