www.computeria-olten.ch
Monatstreff für Menschen ab 50

Merkblatt 157

Die fiesesten Tricks der Virenschreiber

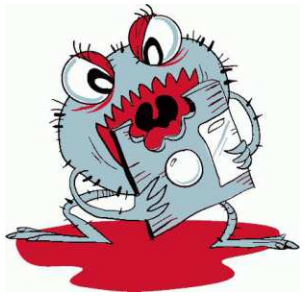
9.9.2019, Ernst Fluri

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.

Nichtsahnende Computernutzer können Backdoor-Programme unbeabsichtigt mit E-Mail-Anhängen und File-Sharing-Programmen herunterladen. Die Autoren geben den Dateien vertrauenserweckende Namen und überlisten so zu ihrem Öffnen und Ausführen.

Bootviren



Sie verändern den Startbereich von Disketten und Festplatten. Das kann beispielsweise den Start des Betriebsprogramms verhindern. Ein Bootvirus ist ein Computervirus, das beim Start des Rechners aktiv wird, noch bevor das Betriebssystem komplett geladen ist.

Auf Disketten, Sticks usw. sitzt das Virus zumindest teilweise im Bootsektor; selbst Disketten, die keine Dateien enthalten, können also infiziert sein.

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."

Ein Virus-Hoax (Hoax: Schwindel, Betrug) ist eine gefälschte Warnung vor einem Computervirus. Normalerweise werden diese Warnungen per E-Mail oder über Nachrichten in einem internen Unternehmensnetzwerk verbreitet. Diese Nachrichten breiten sich meistens wie ein Kettenbrief aus. Die Empfänger sollen sie ebenfalls an ihre Bekannten weiterleiten.

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.

Besondere Vorsicht ist bei der Nutzung öffentlich zugänglicher Rechnern geboten. Vermeiden Sie grundsätzlich die Eingabe vertraulicher Daten auf öffentlichen Rechnern.

Rootkit

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

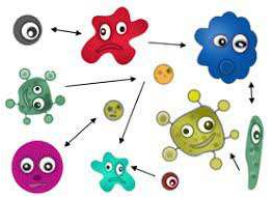
Rootkits können auf verschiedene Weise installiert werden, z. B. auch durch kommerzielle Sicherheitsprodukte und scheinbar sichere Erweiterungen von Drittherstellern.

Makroviren

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 Dokumenten übertragen und Daten verändern oder löschen.

Makroviren werden in der Regel in Dokumente eingebettet oder als schädlicher Code in Textverarbeitungsprogramme eingefügt. Sie können auch als E-Mail-Anhang versendet werden oder durch Klicken auf manipulierte URLs in das System eingeschleust werden. Makroviren sind schwer zu erkennen, da sie erst mit der Ausführung eines infizierten Makros in Aktion treten.

Polymorphe Viren



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

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.

Spyware kommt oft im Paket mit anderer Software oder mit Downloads von File-Sharing-Websites (z. B. Websites für Gratis-Musikdownloads oder mit Filmen), oder sie wird beim Öffnen von E-Mail-Anhängen installiert. Da Spyware im Verborgenen arbeitet, wissen die meisten Anwender gar nicht, dass sich Spyware auf ihren Computern befindet.

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.

Bei einem Trojaner handelt es sich um ein Schadsoftwareprogramm, das in anderen Programmen enthalten ist. Es gelangt über ein zulässiges Programm, beispielsweise einen Bildschirmschoner, auf den Computer.

Wie kommen Viren auf den Computer?

- Die einfachste Art und Weise, auf die Hacker die Computer von Usern infizieren können, ist mit einem USB-Stick.
- Da aber die wenigsten Hacker direkten Zugriff auf den Computer ihres Opfers haben, nutzen diese andere Methoden, um ihre Schadsoftware zu verbreiten.
- Es können Anhänge in E-Mails sein.
- Unter anderem werden dafür gefälschte Websites benutzt, die dem User kostenlose Programme verspricht – allerdings Viren verbreiten.
- Außerdem fängt man sich beim Aufruf diverser Erotik- und Streaming-Seiten schnell einen Virus ein – genauso wie bei dem „kostenlosen“ Download von Filmen, Musik oder Spielen.
- Es gibt auch Websites, die dem Benutzer vorgaukeln, sein Rechner sei infiziert – und beim Download eines „Antivirenprogramms“ erfolgt dann die eigentliche Infektion.

Grundsätzlich sei gesagt, dass die Methoden der Hacker zu vielzählig sind, um sie alle hier aufzuzählen.

Jedoch ist man immer auf der sicheren Seite, wenn man zusätzlich zu seinem Hirn auch ein gutes Antivirenprogramm an seiner Seite hat.