



Spionagesoftware

Spionagesoftware (auch Spähprogramme oder Spyware) sind Schadprogramme, die Daten eines Computers und das Suchverhalten eines Internetnutzers ohne sein Wissen auslesen, analysieren und an Dritte weiterleiten.

Einsatz von Spähprogrammen

Spionagesoftware dient dazu, das Nutzerverhalten im Internet zu verfolgen und Daten auszulesen, wie etwa im Browser gespeicherte Passwörter. Spähprogramme werden in den unterschiedlichsten Bereichen eingesetzt mit dem Ziel, Informationen zu sammeln, auszuwerten und sie für eigene Zwecke zu nutzen. Mit Hilfe von Spyware können zum Beispiel nutzerspezifische Vorlieben erfasst und so Online-Werbung gezielter platziert werden. In Firmennetzwerken kann mit Spionagesoftware überwacht werden, wie Mitarbeiter Computer und das Internet nutzen.

Funktionsweise

Spionagesoftware kann gezielt von jemandem auf Computern und in Netzwerken installiert werden. In den meisten Fällen gelangt sie jedoch durch aufgerufene Internetseiten auf PCs und Smartphones. Dies geschieht über die „Aktiven Inhalte“ einer Webseite. Das sind verborgene Funktionen, die über den Browser auf dem Computer ausgeführt werden, wie JavaScript oder Flash. Über diese kann die Spyware installiert werden. Wird der PC hochgefahren, wird auch das Programm im Hintergrund gestartet. Sobald eine Internetverbindung besteht, werden die gesammelten Informationen versendet. Die Schadsoftware kann aber auch Einstellungen verändern wie die Browser-Startseite. Das Bundesamt für Sicherheit und Informationstechnik warnt insbesondere vor so genannten Keyloggern. Das sind Spyware-Programme, die Tastatureingaben und andere Aktivitäten am Computer überwachen.

Symptome

Indizien dafür, dass auf einem Computer Spionagesoftware installiert ist, sind:

Der Computer verbindet sich eigenständig mit dem Internet.

Die Browser-Startseite und gespeicherten Favoriten wurden verändert.

Das Surfen im Internet funktioniert nur noch sehr langsam.

Im Browser öffnen sich Werbefenster, die in keinem Zusammenhang mit besuchten Webseiten stehen.

Es gibt auch zahlreiche Programme, mit denen Spionagesoftware ausgemacht werden kann.

Schutz vor Spähprogrammen

Um das Risiko zu senken, dass sich ein Spähprogramm auf dem Computer installiert, sollten nur vertrauenswürdige Links auf Webseiten oder in E-Mails geöffnet werden. Besonders schwer zu erkennen ist dies bei Links, die mit einem URL-Shortener verkürzt wurden, weil hierbei nicht zu sehen ist, auf welcher Webseite man landet. Das Installieren von Cookies sollte „nur von besuchten“ Seite akzeptiert werden. Diese Einstellung kann im Browser gewählt werden. Auch das Ausführen von aktiven Inhalten kann hier unterbunden werden. Der Browser und das Betriebssystem sollten regelmäßig aktualisiert werden. Es empfiehlt sich zudem die Verwendung einer Firewall, von Virenscannern und Anti-Spyware-Programmen.

Spyware der Geheimdienste

Der Amerikaner Edward Snowden enthüllte im Juni 2013, wie die USA (der Geheimdienst NSA) und Großbritannien die Telefone und das Internet global überwachen und die Daten speichern. Neben Bürgern wurden auch Botschaften, EU-

Vertretungen und die Zentrale der Vereinten Nationen ausspioniert. Es waren Programme wie PRISM, Tempora, XKeyscore, Fairview und Boundles Informant im Einsatz sowie das „Mail Isolation Control and Tracking“-Programm. Zudem sollen Unterseeglasfaserkabel angezapft worden sein.

Siehe auch:

[Trojanisches Pferd](#)

[Antivirensoftware](#)

[Zurück](#)

© Verlag Deutsche Polizeiliteratur