Botnetz

Botnetze entstehen, wenn Internetkriminelle bis zu mehrere Millionen PCs per Fernsteuerung ohne das Wissen ihrer Nutzer zusammenschließen, um zum Beispiel Spam-Mails zu verschicken oder einen Server durch massenhafte Anfragen lahmzulegen (DDos-Attacken).

Wenn PCs zu Zombies werden

Die Schadprogramme werden beispielsweise durch das Öffnen von E-Mail-Anhängen unbekannter Absender auf die Festplatten der Computer geschleust. Auch der Besuch entsprechend präparierter Webseiten kann dazu führen, dass sich ein Schadprogramm ohne Wissen des PC-Nutzers installiert. Außerdem nutzen die Schadprogramme Schwachstellen in Betriebssystemen aus, um fremde Computer zu infizieren. Auch Server werden auf diese Weise instrumentalisiert. Internetkriminelle steuern diese Armee sogenannter „Zombies“ dann zentral und können so rechenintensive Leistungen durchführen, mit denen sie beispielsweise Webseiten komplett lahmlegen oder Spam-Mails versenden. Im Gegensatz zu analogen Internetverbindungen fällt bei den heutigen schnellen DSL-Anschlüssen kaum auf, ob ein Computer an ein Botnetz angeschlossen ist, weil die Verbindungsgeschwindigkeit durch die im Hintergrund ablaufenden Rechenvorgänge nicht merklich langsamer wird.

Schutzmaßnahmen

Damit ein Computer nicht Teil eines Botnetzes wird, sollte man ein Antivirenschutz-Programm sowie eine Firewall auf dem Rechner installieren und diese immer auf dem neuesten Stand halten. Außerdem sollte man Mailanhänge unbekannter Absender in aller Regel nicht öffnen, sondern diese Mails umgehend löschen. Mehr Informationen zu Botnetzen findet man auch im Portal BSI für Bürger des Bundesamts für Sicherheit in der Informationstechnik.

Siehe auch:
Antivirensoftware
Malware/Spyware
Skimming

Zurück