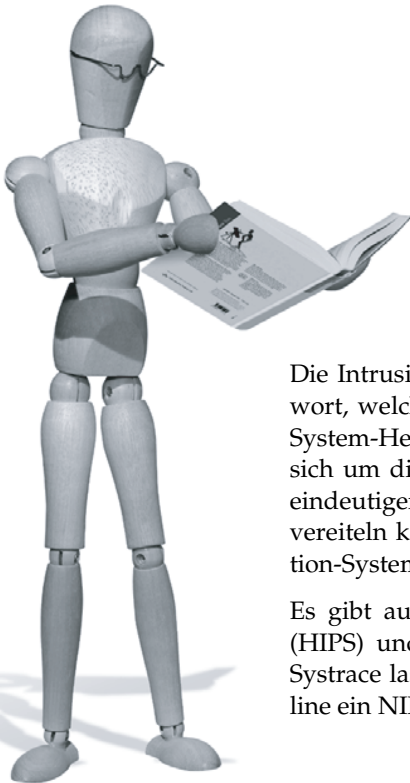


Teil III

Verfügbare Open-Source-Intrusion- Prevention-Systeme



Die Intrusion Prevention ist ein noch relativ neues Modewort, welches vor 2-3 Jahren von den Intrusion Detection System-Herstellern erfunden wurde. Hierbei handelt es sich um die Idee, dass ein Intrusion-Detection-System bei eindeutiger Erkennung eines Einbruchs diesen auch gleich vereiteln könnte. Diese Systeme werden Intrusion-Prevention-Systeme (IPS) genannt.

Es gibt auch hier grundsätzlich zwei Ansätze: Host IPS (HIPS) und Network IPS (NIPS). Sowohl LIDS als auch Systrace lassen sich als HIPS einsetzen, während Snort-Inline ein NIPS ist.

