

Teil I

Einführung in die Intrusion Detection



Die Computersicherheit ist eine recht junge Wissenschaft. Ihre Anfänge liegen in den siebziger Jahren des 20. Jahrhunderts. Die Intrusion Detection ist ein Teilbereich der Computersicherheit. James P. Anderson veröffentlichte im Oktober 1972 einen ersten Artikel, der sich mit der Computersicherheit beschäftigte (<http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf>). Er beschreibt in diesem Artikel die Sicherheitsprobleme bei der US Air Force als deren Angestellter. April 1980 konkretisierte er die Probleme und entwickelte Verfahren zur Überwachung dieser Sicherheitsprobleme (<http://seclab.cs.ucdavis.edu/projects/nsotry/papers/ande80.pdf>). Dieser Artikel beschreibt verschiedene Möglichkeiten zum Audit von Computern. Diese stellen somit den Beginn der Überwachung und der Intrusion Detection dar. In den achtziger Jahren wurden von der amerikanischen Regierung verschiedene Projekte zur Entwicklung und Erforschung der Intrusion-Detection-Systeme

(IDS) gestartet. Die bekanntesten sind wahrscheinlich das *Multics Intrusion Detection and Alerting System (MIDAS)*, der *Network Audit Director and Intrusion Reporter (NIDAS)* und der *Network System Monitor (NSM)*. Der NSM war 1989 das erste Network-IDS. Ende der achtziger Jahre und Anfang der neunziger wurden die ersten kommerziellen IDS auf dem Markt verfügbar.

Da die Intrusion Detection ein derartig neues Feld darstellt, welches erst in den letzten fünf bis zehn Jahren kommerzielles Interesse findet, sollen im Folgenden wichtige Grundlagen erklärt und Begriffe bestimmt werden. Dies sind scheinbar so einfache Begriffe wie die *Intrusion* selbst, wie auch einige Ausführungen zum Datenschutz bei Einsatz eines IDS.