Intrusion Detection & Response

Seminararbeit im SS 2002 (4. Semester Bachelor)

von

Uwe Hoffmeister – 900 1840

Christian Klie – 900 1882

Tobias Schmidt – 900 1883

1. Verzeichnisse

1.1. Inhaltsverzeichnis

1.2. Tabellenverzeichnis

1.3. Abbildungsverzeichnis

1.4. Abkürzungsverzeichnis

ACK	acknowledgement flag
ASCII	American standard code for information interchange
bzw	beziehungsweise
CDIR	Classes InterDomain Routing
CGI	commen gateway interface
CPU	central processing unit
FIN	Final Flag
GRE	Generic Route Encapsulation
HTTP	hypertext transport protocol
HTTPS	hypertext transport protocol secure
ICMP	internet control management protocol
ID	identification
IDS	Intrusion Detection System
IGRP	interior gateway routing protocol
IP	Internet Protocol
IPX	internet packet exchange protocol
IT	Informations Technologie
OSPF	open shortest path first
RIP	routing information protocol
RSH	remote shell
RST	Reset Flag
SMTP	simple mail transfer protocol
SYN	synchronization
TCP	Transfer Control Protocol
UDP	user datagram protocol
URL	uniform resource locator
XML	Extensible Markup Language
z.B.	zum Beispiel

2. Allgemeine Einführung ins Thema

Die Sicherheit von IT- Systemen ist in den letzten Jahren zusehends gestiegen. Gründe hierfür liegen zum einen in der globalen Vernetzung von Rechnersystemen und einer immer komplexer werdenden Softwarearchitektur. Als schützenswert erweist sich nicht nur das interne Firmennetz gegenüber Angriffen aus dem eigenen Netz, sondern im zunehmenden Maße auch der Schutz gegen externe Angriffe.

Seitdem IT- Systeme existieren, gibt es Bemühungen, die zum Ziel den Schutz dieser Systeme haben. Allerdings gibt es immer wieder Möglichkeiten, diese Schutzmaßnahmen zu umgehen. Das Interesse an flexiblen und schnell agierenden Systemen zum Schutz von IT-Systemen ist in den letzten Jahren stark gestiegen. Aus diesem Grund, werden Intrusion Detection/ Intrusion Response Systeme entwickelt, um die benötigte Sicherheit zu gewährleisten.

Vorläufer und Basis von Intrusion Detection/ Intrusion Response Systemen sind Auditsysteme, die alle Vorgänge innerhalb eines IT- Systems aufzeichnen und deren Protokolle nachträglich ausgewertet werden. Der Vorteil von Intrusion Detection/ Intrusion Response Systemen liegt in der zeitnahen Auswertung von Auditfiles, um Entscheidungen treffen zu können, die das IT- System sichern.

Diese Arbeit beschäftigt sich mit Intrusion Detection Systemen, Angriffen auf Rechnersysteme und mit einer Möglichkeit zur Intrusion Response/Reactive.