



1 Computersicherheit

1.1 Übersicht

In diesem einleitenden Kapitel möchte ich Ihnen einige Hintergründe zum Thema Computersicherheit liefern. Hierbei soll es sich aber nur um kurze Einführungen handeln, die in keiner Weise erschöpfend sind.

Allgemein beschreiben vier grundlegende Begriffe die *Informationssicherheit*. Diese sind zum Teil sogar in einem Standard festgelegt (ISO 17799, BS 7799). Da Computer Informationen (Daten) verarbeiten, können diese Begriffe direkt auf die Computersicherheit übertragen werden:

- Confidentiality
- Integrity
- Availability

Diese Begriffe will ich kurz erläutern. Die *Confidentiality* beschreibt die *Vertraulichkeit* der Daten. *Vertraulichkeit* ist eines der vier wichtigsten Sachziele in der Informationssicherheit. Sie beschreibt die Eigenschaft eines Systems, berechtigten Subjekten den Zugriff auf bestimmte Objekte (häufig elektronische oder physische Dokumente) zu gestatten und unberechtigten Subjekten den Zugriff auf diese Objekte zu verwehren.

Unter Vertraulichkeit versteht man, dass eine Information nur für Befugte zugänglich ist, Unbefugte dagegen keinen Zugang zu der Information haben. So können beispielsweise nur der Sender und der Empfänger eine Nachricht im Klartext lesen.

Die *Integrity* (*Integrität*) beschreibt die Tatsache, dass Daten über einen bestimmten Zeitraum vollständig und unverändert sind. Eine Veränderung könnte absichtlich, unabsichtlich oder durch einen technischen Fehler auftreten.

Die *Integrität* von Daten ist also gewährleistet, wenn die Daten vom angegebenen Absender stammen und vollständig sowie unverändert an dem Empfänger übertragen worden sind.

Die *Availability* oder auch *Verfügbarkeit* bezeichnet die Fähigkeit, auf die benötigten Daten jederzeit zugreifen zu können. Sie wird daher sowohl durch die Zuverlässigkeit des Systems, das die Daten zur Verfügung stellt, als auch durch die Erreichbarkeit des Systems bestimmt.

Zusätzlich zu diesen drei Hauptzielen gibt es auch noch drei weitere Ziele, die hier nur kurz erwähnt werden sollen: Authentizität, Nichtabstreitbarkeit und Verbindlichkeit. Im Weiteren will ich auf diese jedoch nicht mehr eingehen.

Allgemein werden diese Schutzziele bedroht. So kann es zu unautorisiertem Zugang kommen, falsche Daten können vorgetäuscht werden, oder der Zugang zum System kann verhindert werden. Um diesen Bedrohungen zu begegnen, ist es zunächst erforderlich, diese genau zu ermitteln und dann eine *Security-Policy* (*Sicherheitsrichtlinie*) zu erzeugen, die beschreibt, was erlaubt und was verboten ist. Hierauf kann dann ein Sicherheitsmechanismus aufbauen und die Umsetzung der Sicherheitsrichtlinie erzwingen.

Computerbetriebssysteme verfügen seit vielen Jahren über die unterschiedlichsten Sicherheitsmechanismen, die die Umsetzung von Sicherheitsrichtlinien erlauben. Hierbei handelt es sich meist um Discretionary-Access-Control-Systeme¹. In einigen Umgebungen genügen diese einfachen Sicherheitsmechanismen nicht. Die hier gewünschten Security Policies erfordern umfangreichere und komplizierte Sicherheitsmechanismen. Hierzu gehören zum Beispiel militärische Anwendungen mit sehr hohen Geheimhaltungsanforderungen. Novell AppArmor und SELinux sind zwei konkurrierende Systeme, die derartige Security Policies umsetzen können. Dieses Buch beschäftigt sich mit der Erzeugung, Administration, Anpassung und Wartung dieser Security Policies.

1.2 Anfänge der Computersicherheit

In diesem Kapitel stelle ich kurz die Geschichte der Computersicherheit in den letzten 40 Jahren dar. Computersicherheit wird erst seit den 70er-Jahren tatsächlich untersucht, obwohl auch frühere Systeme, wie MULTICS und Atlas davon beeinflusst wurden.

Die folgende Darstellung basiert unter anderem auf der Zusammenstellung von Dokumenten durch Matt Bishop vom Computer Security Laboratory der Universität von Kalifornien in Davis (UCD). Diese ist im Internet unter <http://csrc.nist.gov/publications/history/> zu finden.

1969 beschrieb Butler Lampson [4] bereits die Grundlagen moderner Zugriffskontrollsysteme. Von ihm wurden die Begriffe Capability und Domain erstmals beschrieben. 1970 legte Willis H. Ware [8] die Grundlagen für Multi-Level-Security-Systeme und beschrieb erstmals die Anforderungen an Betriebssysteme, wenn mehrere Benutzer Daten unterschiedlicher Sensitivität verarbeiten. 1972 erweiterte James P. Anderson [9] das Multi-Level-Modell von Ware in einer Studie für die United States Air Force. Im Jahr 1973 legten David E. Bell und Leonard J. LaPadula [10] mit ihrem Dokument »Secure Computer Systems: Mathematical Foundations« die Grundlagen für das Bell-LaPadula-Modell. Dies ist bis heute das bekannteste Multi-Level-Security-Modell. Dieses Modell wird in Abschnitt 2.1.3 genauer erläutert. 1974 defi-

¹ Was das ist, wird in Abschnitt 1.2 erklärt.

nierte Butler Lampson das Referenzmonitor-Modell. Dieses, auch als Zugriffsmatrix bekannte Modell, beschreibt anhand einer Matrix, wie ein Subjekt auf ein Objekt zugreifen darf.

1979 legten Peter G. Neumann et al. die Grundlagen für ein »Provably Secure Operating System (PSOS)« [11]. Dieses stellte später die Grundlage für das Betriebssystem LOCK dar, das 1987 von O. Sami Saydjari et al. vorgestellt wurde [12]. Dieses Betriebssystem führt als erstes das Type-Enforcement ein. 1987 versuchten Clark und Wilson [5] das Bell-LaPadula- und das Biba-Modell auf kommerzielle Systeme zu übertragen. Der wesentliche Aspekt dieses Modells ist die Integritätsicherung. Damit lässt sich das Clark-Wilson-Modell gut auf Geschäftsprozesse übertragen.

1992 beschrieben Ferraiolo und Kuhn [13] das Role-Based-Access-Control-Modell. Dieses wurde in den folgenden Jahren weiterentwickelt ([14, 15]) und von dem National Institute for Standards and Technology (NIST) standardisiert (American National Standard 359-2004).

