

Kapitel 1

Einleitung

1.1 Motivation

Ein wichtiger Bestandteil der heutigen IT-Landschaft ist der Bereich der IT-Sicherheit, der sich mit den Gefährdungen für und durch IT-Systeme beschäftigt. Ein Grund für das konstante Wachstum dieser Branche in den vergangenen Jahren sind die zahlreichen Sicherheitslücken aktueller IT-Systeme, die zu einer globalen Verbreitung von Schadsoftware (wie z. B. Viren, Würmer, Trojanische Pferde und Spyware) auf Computern von Privatpersonen und Unternehmen führen. Die Ausnutzung von Sicherheitslücken von IT-Systemen ist grundsätzlich keine neue Erscheinung der Computerbranche, jedoch ist in den letzten Jahren eine deutliche Zunahme im Bereich der finanziell motivierten Internetkriminalität zu erkennen. So enthielt anfangs ein Großteil der heute als Schadsoftware bezeichneten Programme keine wirkliche Schadfunktion, sondern diente vielmehr der Demonstration einer Sicherheitslücke (*Proof-of-Concept*) zur Sensibilisierung für die daraus entstehenden Gefahren. Die Hauptaufgabe heutiger Schadsoftware ist meist der Aufbau einer technischen Infrastruktur für die organisierte Internetkriminalität. Typische Schadfunktionen hierbei sind das Ausspähen von privaten Daten (z. B. Passwörter, Kreditkartennummern, Softwarelizenzen), der Aufbau von zentral gesteuerten Rechnernetzwerken (Bot-Netze) zum Versand von Spam oder zum großflächigen Angriff auf die Verfügbarkeit einzelner Systeme (DDoS¹) sowie die automatische Suche nach weiteren Systemen mit dieser Sicherheitslücke zur eigenen Replikation. Ein weiterer aktueller Trend ist im Wandel hin zu sehr gezielten Angriffen auf die Infrastruktur eines einzelnen Unternehmens mit dem primären Ziel der Wirtschaftsspionage zu erkennen. Schätzungen der Hersteller von Virenschutzsoftware zufolge sind aktuell zwischen 50% und 90% aller mit dem Internet verbundenen Computer mit einer oder mehreren Arten von Schadsoftware infiziert. Diese Infrastruktur ermöglicht der so genannten *Underground Economy*² die einfache und nahezu risikofreie Erschließung eines neuen Marktsegments. Nach Aussage des US-

¹ DDoS – Distributed-Denial-of-Service-Angriffe

² [URL01]

Finanzministerium liegt der jährliche durch die Internetkriminalität erzeugte Umsatz oberhalb von 100 Milliarden US-Dollar und beläuft sich damit auf mehr als im weltweiten Drogenhandel jährlich umgeschlagen wird³.

Unterstützt wird die Verbreitung von Schadsoftware durch die nahezu flächendeckende Verfügbarkeit von breitbandigen Internetzugängen für private Haushalte. Der eigentliche Ursprung jedoch liegt in den Sicherheitslücken der eingesetzten Betriebssysteme und Anwenderprogramme. Speziell die Betriebssysteme konnten mit der rasanten Weiterentwicklung bei den Techniken für Schadsoftware nicht Schritt halten. So basieren zum Beispiel die in aktuellen Desktop-Betriebssystemen implementierten Zugriffskontrollsysteme immer noch auf den zu Beginn der PC-Ära entwickelten Konzepten. Zu diesem Zeitpunkt war der PC überwiegend ein Single-User-System ohne Zugriff auf ein öffentliches Netzwerk wie das Internet. Ein weiteres Manko heutiger Betriebssysteme ist die Verwendung von unsicheren Programmiersprachen (wie z. B. C und C++) für deren Entwicklung. Die dabei häufig auftretenden Fehler bei der Programmierung bilden den Angriffsvektor (z. B. durch Buffer Overflows) für das Einschleusen von Schadcode in das Betriebssystem oder in eine Applikation.

Um die Anzahl möglicher Angriffsvektoren zu reduzieren oder deren Auswirkung auf die Systemintegrität abzuschwächen, wurden in der nahen Vergangenheit unterschiedliche neue Konzepte entwickelt. Hinter dem Begriff *Trusted Computing* verbirgt sich eines dieser Konzepte zur Verbesserung der Computersicherheit. Dieses Buch beschäftigt sich ausführlich mit den Konzepten und Anforderungen dieser noch verhältnismäßig jungen Technologie.

1.2 Ziele des Buches

Das Schlagwort *Trusted Computing* ist immer häufiger das Thema von Fachartikeln, Internetbeiträgen und sogar ganzen Konferenzen und Workshops. Der Begriff ist inzwischen auch bei Personen außerhalb der IT-Sicherheitsbranche bekannt, wenn auch überwiegend auf Grund einer gewissen Nähe zum Thema *Digital Rights Management* (DRM).

Trotz der erlangten Aufmerksamkeit und der verfügbaren Publikationen ist es selbst für Fachleute auf dem Gebiet der IT-Sicherheit schwierig, sich einen klaren Überblick über diese Technologie zu verschaffen. Dies liegt darin begründet, dass sich viele der Artikel nur mit einem kleinen Teilbereich der Technologie beschäftigen, den Leser aber häufig über diesen Missstand nicht informieren. So wird das Thema *Trusted Computing* oft auf das im Zuge der Entwicklungen eingeführte *Trusted Platform Modul* (TPM) und dessen Funktionen beschränkt. Weiter ist zum Zeitpunkt der Entstehung dieses Buches keine Grundlagenliteratur zum Thema *Trusted Computing* verfügbar.

³ [URL02]



<http://www.springer.com/978-3-540-76409-0>

Trusted Computing Systeme
Konzepte und Anforderungen

Müller, Th.

2008, XV, 160 S., Hardcover

ISBN: 978-3-540-76409-0