

# Vorwort

*Tunneling und verdeckte Kanäle* – was hat es damit auf sich?

Beide Themen sind in der heutigen IT-Welt von großer Bedeutung. Tunnel ermöglichen die Kommunikation durch praktisch beliebige Netzwerke und sind insbesondere für den Umstieg auf IPv6 von elementarer Bedeutung. Verdeckte Kanäle können etwa Journalisten und der politischen Opposition in Ländern mit Internetzensur helfen, sicher regimekritische Informationen zu übertragen. Auf der anderen Seite dienen verdeckte Kanäle auch der Exfiltration geheimer Unternehmensdaten und sollten daher nach Möglichkeit administrativ unterbunden werden, um den Diebstahl von Know-How zu verhindern.

*Welches Ziel verfolgt dieses Buch?*

Es soll Studenten der höheren Semester sowie Professionals eine Einführung in die Thematik des Tunnelings und der verdeckten Kanäle geben. Dabei unterscheiden sich beide Teile des Werks in ihrer Zielsetzung: Während der erste Teil kurz die Grundlagen der modernen Netzwerke wiederholt (Kapitel 2), führt Kapitel 3 in alle gängigen Tunnelingverfahren ein und soll so einen Überblick und ein Verständnis für das Tunneling ermöglichen. Erst auf dieser Grundlage sind auch Konfigurationen in der Praxis realisierbar (diese sind allerdings sehr von System und Use-Case abhängig und können daher im Umfang des Titels nicht abgedeckt werden). Im zweiten Teil des Titels wird hingegen eine Einführung in das geheime Tunneling und die Forschungsthematik der verdeckten Kanäle vorgenommen. Doktoranden, Wissenschaftlern und Masterstudenten sollen die aktuellen Forschungsthemen der verdeckten Kanäle erläutert werden.

H.G. Eßer veröffentlichte bereits zuvor ein Buch im Themenfeld, konzentrierte sich dabei allerdings ausschließlich auf verdeckte *Zeitkanäle* (*timing channels*) und zudem auf den speziellen Kontext von Web-Services. Ich empfehle sein Buch für die zusätzliche Auseinandersetzung mit Zeitkanälen.

Das vorliegende Werk ist folglich das erste, welches verdeckte Kanäle ganzheitlich betrachtet. Es basiert auf meiner jahrelangen intensiven Auseinandersetzung mit dem Thema. Große Teile dieses Buches basieren auf meiner Diplomarbeit an der Hochschule Kempten (zwei Abschnitte aus Kapitel 4, Details in Kapitel 7), auf meiner Masterarbeit an der Hochschule Augsburg (Kapitel 6) und auf meiner bisherigen Doktoratszeit an der FernUniversität in Hagen (Kapitel 7). Kapitel 2 basiert zum Großteil auf dem Anhang des »Praxisbuch Netzwerksicherheit« von 2007, wurde allerdings erweitert, aktualisiert und freundlicher Weise vom Galileo Press-Verlag zur Publikation in diesem neuen Buch freigegeben.

## Dank

Frau Christel Roß, Herrn Bernd Hanseman und Frau Maren Mithöfer danke ich für die Betreuung des Buchprojekts und dafür, dieses Buch durchgesetzt zu haben. Ich danke Judith Stevens-

Lemoine (Galileo Press) für die Möglichkeit, Inhalte aus unserem alten »Praxisbuch Netzwerksicherheit« (2. Aufl., 2007) in diesem Buch verwenden zu dürfen.<sup>1</sup> Übernommene Inhalte (dies betrifft nur Teile von Kapitel 2 und einen Abschnitt aus Kapitel 3) habe ich selbstverständlich einer Aktualisierung und einer Erweiterung unterzogen.

Bei der fachlichen Durchsicht des Manuskripts durfte ich auf die Unterstützung von Jörg Keller, Sebastian Schinzel und Sebastian Zander zurückgreifen, die jeweils unterschiedliche Abschnitte durchsahen. Vielen Dank an dieser Stelle! Sollte dieses Buch dennoch Fehler beinhalten, so ist der Grund dafür allein bei meiner Person zu suchen.

Ich wünsche allen Lesern bei der Auseinandersetzung mit diesem sowohl praktischen, als auch akademischen Thema viel Freude. Konstruktives Feedback zum Buch ist explizit erwünscht.

Augsburg im Mai 2012

Steffen Wendzel  
<http://www.wendzel.de>

## Über den Autor

Steffen Wendzel ist Autor mehrerer Fachbücher. Er studierte Informatik mit Schwerpunkt Netzwerktechnik, Betriebssysteme und Wirtschaftsinformatik an der Hochschule Kempten und Informatik mit Schwerpunkt der sicheren Netzwerke an der Hochschule Augsburg. Derzeit finalisiert er seine Doktorarbeit zu einem Spezialbereich der verdeckten Kanäle am Lehrstuhl für Parallelität und VLSI an der FernUniversität in Hagen. Weiterhin ist Herr Wendzel als wissenschaftlicher Mitarbeiter im Rahmen von Lehre und Forschung an der Hochschule Augsburg tätig.

## Aufbau dieses Buches

Nach einem einführenden Kapitel, in dem verschiedene Begrifflichkeiten erläutert werden, führt Kapitel 2 in die Grundlagen von TCP/IP insofern ein, als sie für das Verständnis der folgenden Kapitel von Belang sind.

Kapitel 3 behandelt *legitime* Tunnelingverfahren. Dabei werden insbesondere verschiedene Protokolle vorgestellt, die für den Umstieg von IPv4 auf IPv6 von Bedeutung sind. Kapitel 4 betrachtet hingegen das *nicht legitime*, geheime Tunneling, wie es von der Hacking-Community seit Mitte der 90er und parallel in der wissenschaftlichen Community Ende der 80er Jahre betrachtet wurde. Die dort vorgestellten Verfahren sind folglich tatsächlich bereits verdeckte Kanäle, aber auch ohne den wissenschaftlichen Kontext derselben vollständig zu verstehen.

Genau dieser wissenschaftliche Kontext wird in Kapitel 5 eingeführt, woraufhin Kapitel 6 die Detektions- und Präventionsmethoden für verdeckte Kanäle behandelt, die in den letzten Jahrzehnten innerhalb der Forschung entwickelt wurden. Abschließend gibt Kapitel 7 einen Einblick in die fortgeschrittenen Themen der verdeckten Kanäle und betrachtet dabei insbesondere Ergebnisse eigener Forschungsarbeiten.

---

<sup>1</sup> Das Praxisbuch Netzwerksicherheit ist nur noch antiquarisch erhältlich.

Tunnel und verdeckte Kanäle im Netz  
Grundlagen, Protokolle, Sicherheit und Methoden  
Wendzel, S.  
2012, VIII, 179 S. 57 Abb., Softcover  
ISBN: 978-3-8348-1640-5