Vorwort

Der gegenwärtige Wandel zur Informations- und Wissensgesellschaft verändert unser Leben – und damit auch das Wirtschaftsleben – tief greifend. Die »elektronische Geschäftswelt« bietet uns neue Chancen, denen jedoch, ähnlich wie in der »traditionellen Geschäftswelt«, bestimmte Risiken gegenüberstehen.

In der »traditionellen Geschäftswelt« haben wir im Laufe der Zeit gelernt, diese Risiken einzuschätzen und uns angemessen dagegen zu schützen: Schutzmechanismen wie Pförtner, Safes und gepanzerte Werttransporter, aber auch Ausweise, Briefumschläge und die eigenhändige Unterschrift gewährleisten zwar keine hundertprozentige Sicherheit, aber sie helfen, das Risiko auf ein kalkulierbares Maß zu begrenzen.

Entsprechende Mechanismen benötigen wir auch in der »elektronischen Geschäftswelt«. Damit wir die Möglichkeiten, die uns die Kommunikation über das Internet bietet, erfolgreich nutzen können, müssen die grundlegenden Sicherheitsanforderungen – *Vertraulichkeit, Authentizität, Integrität* und *Nachweisbarkeit* von Datenübertragungen – erfüllt werden.

Diese Notwendigkeit wird um so deutlicher, wenn wir den immer weiter steigenden Wert elektronischer Informationen in Betracht ziehen. Immer mehr Daten, die erhebliche finanzielle Werte darstellen, werden durch Netze übertragen oder auf Rechnersystemen gespeichert. Dazu gehören Entwicklungsunterlagen, Kundendaten, Logistikinformationen oder auch Strategiekonzepte, die möglicherweise Börsenwerte beeinflussen können. Die Bits und Bytes solcher Informationen können leicht mehrere Millionen Euro wert sein.

Hinzu kommt, dass die gegenwärtige, national begrenzte Gesetzgebung im weltweiten Internet keinen angemessenen Schutz bieten kann. Es wird sicher noch Jahre dauern, bis internationale Gesetze – z. B. im Rahmen der G8-Bemühungen – erlassen werden. Bis dahin müssen Unternehmen und Organisationen sich mit geeigneten IT-Sicherheitsmaßnahmen selbst gegen die Gefahren der »elektronischen Welt« schützen.

Ein Beispiel für solche Sicherheitsmaßnahmen sind *Virtual Private Networks (VPNs)*, mit denen unsichere Netze wie das Internet als vertrauenswürdige Kommunikationswege genutzt werden können – ähnlich wie auch das Straßennetz von gesicherten Geldtransportern befahren wird.

Unter dem Begriff »VPN« werden Hard- und Software-Lösungen zusammengefasst, die sich in ihren Einsatzgebieten und ihrer technischen Realisierung deutlich unterscheiden. Dieses Fachbuch soll zur Klärung des Begriffs beitragen und stellt die grundlegenden Konzepte von VPN-Systemen dar. Als praxisorientierter Leitfaden erläutert es verschiedene Einsatzmöglichkeiten von VPNs und bietet den Lesern Hilfestellungen zur Wirtschaftlichkeitsberechnung, zur Definition einer VPN-Sicherheitspolitik sowie zu Beschaffung, Instandhaltung und Betrieb von VPN-Systemen.

Für die zweite Auflage wurde das Buch erneut durchgesehen und an verschiedenen Stellen aktualisiert oder ergänzt.

Unser Dank gilt den VPN-Spezialisten der Compumatica secure networks GmbH. Unsere Leser sind weiterhin gerne eingeladen, Fragen zu stellen und Anregungen zu geben. Sie erreichen uns dazu per E-Mail unter:

Dr.-Ing. Markus a Campo: mail@m-acampo.de

Dr. Norbert Pohlmann: norbert.pohlmann@utimaco.de