1 Einleitung

Es ist eine mittlerweile wohlbekannte Tatsache, dass die digitale Revolution und die allgegenwärtige Vernetzung von Informationssystemen bei all ihren Vorteilen auch einige Risiken mit sich bringen. In diesem Buch sind eine bestimmte Kategorie von Risiken und insbesondere die Maßnahmen zu ihrer Bekämpfung von Interesse. Es die Kategorie der Risiken, die aus der Abhörbarkeit und Manipulierbarkeit der in Kommunikationsnetzen übertragenen Daten und der Verwundbarkeit der Kommunikationsinfrastruktur selbst erwachsen.

Schutz zu übertragender Daten

Die Schutzbedürftigkeit zu übertragender, aber auch zu speichernder Daten wurde von der Menschheit schon sehr früh erkannt, und so ist der Wunsch, Daten vor unberechtigtem Zugriff zu schützen, vermutlich so alt wie die Schrift selbst. Verlässliche, frühe Überlieferungen über entsprechende Schutzmaßnahmen berichten beispielsweise über eine von den Spartanern etwa 400 Jahre vor Christus eingesetzte Technik, Nachrichten auf ein Lederband zu schreiben, das um einen Stock eines bestimmten Durchmessers gewickelt war. Vor der Übermittlung der Nachricht wurde das Lederband von dem Stock entfernt, sodass ein potenzieller Angreifer, der nicht über einen Stock des gleichen Durchmessers verfügte (zum Beispiel weil er den Durchmesser oder auch diese Technik nicht kannte), die Nachricht nicht lesen konnte. In gewisser Weise wurde hierdurch eine erste »analoge« Verschlüsselung realisiert.

Erste Substitutionschiffren

Im vierten Jahrhundert vor Christus entwickelte der Grieche Polybius eine Tafel für bilaterale Substitution, die eine Abbildung von Zeichen auf Paare von Symbolen sowie die entsprechende Rückabbildung definierte und somit ein erstes »digitales« Verschlüsselungsverfahren spezifizierte. Von den Römern ist bekannt, dass sie ihre taktische Kommunikation oft mit einfachen, sogenannten monoalphabetischen Substitutionsverfahren schützten, von denen das bekannteste wohl die »Cäsar-Chiffre« sein dürfte. Bei diesem nach seinem Erfinder Julius Cäsar benannten Verschlüsselungsverfahren wird jedes Zeichen des Alphabets auf das um drei Zeichen

folgende Zeichen ersetzt, also etwa »A« durch »D«, »B« durch »E« und so weiter.

Anfänge der Kryptanalyse

Die Araber entwickelten als Erste ein Grundverständnis der beiden fundamentalen Prinzipien *Substitution*, das heißt der Zeichenersetzung, und *Transposition*, welches die Änderung der Reihenfolge der Zeichen eines Textes ist. Sie betrachteten bei der Bewertung von Verfahren auch die Analyse eines Verfahrens durch einen potenziellen Angreifer. So war ihnen bereits die Bedeutung relativer Buchstabenhäufigkeiten einer Sprache für die Analyse von Substitutionschiffren bekannt, da diese Rückschlüsse auf die Substitutionsregeln zulassen. Zu Beginn des fünfzehnten Jahrhunderts nach Christus enthält die arabische Enzyklopädie »Subh al-a'sha« bereits eine beachtliche Abhandlung über kryptografische Verfahren und ihre Analyse.

Schutz der Infrastruktur

Ohne an dieser Stelle die gesamte Entwicklung der Kryptologie zu einer wissenschaftlichen Disziplin nachzuzeichnen, sollte aus den genannten Entwicklungen klarwerden, dass der Schutz zu übertragender Daten seit je her eine besondere Beachtung erfahren hat. Im Zeitalter allgegenwärtiger Kommunikationsnetze erweist sich jedoch zunehmend auch eine zweite Kategorie von Risiken von immer größerer Dringlichkeit, die nicht direkt die zu übertragenden Daten, sondern die Kommunikationsinfrastruktur an sich betrifft. Mit der Entwicklung und dem Ausbau immer komplexerer Netze sowie ihrer zunehmenden Bedeutung – nicht nur für die wirtschaftliche, sondern auch für die soziale Entwicklung einer modernen Informationsgesellschaft – steigen auch die Anforderungen an die Sicherheit der Kommunikationsinfrastruktur vor absichtlichen Manipulationen. So ist für einen wirtschaftlichen Betrieb beispielsweise sicherzustellen, dass die von Kommunikationsnetzen bereitgestellten Dienste zur Verfügung stehen und korrekt funktionieren sowie dass erfolgte Dienstnutzungen auch korrekt und nachvollziehbar abgerechnet werden können.

1.1 Inhalt und Aufbau dieses Buches

In diesem Buch werden die beiden bisher skizzierten Aufgabengebiete der Netzsicherheit, die *Sicherheit zu übertragender Daten* sowie die *Sicherheit der Kommunikationsinfrastruktur*, gleichermaßen behandelt. Hierzu werden in den folgenden Abschnitten zunächst zentrale Begriffe und Konzepte eingeführt und ein erster Überblick über Maßnahmen der Informationssicherheit gegeben.

Teil 1 des Buches behandelt Grundlagen.

In den verbleibenden Kapiteln des ersten Teils werden darauf aufbauend die *Grundlagen der Datensicherheitstechnik* behandelt. Kapitel 2 führt in Grundbegriffe der Kryptografie ein. Kapitel 3 behandelt die Verwendung und die Funktionsweise symmetrischer Chiffrierverfahren. Das sich anschließende Kapitel 4 ist den asymmetrischen kryptografischen Algorithmen gewidmet. Kapitel 5 führt in kryptografische Prüfwerte zur Erkennung von Nachrichtenmanipulationen ein. Die Erzeugung sicherer, nicht vorhersehbarer Zufallszahlen ist Gegenstand von Kapitel 6. Die Algorithmen dieser vier Kapitel stellen gewissermaßen die *Grundprimitive* der Datensicherheitstechnik dar, auf denen die kryptografischen Schutzmechanismen der Netzsicherheit beruhen. Kapitel 7 behandelt kryptografische Protokolle. Hier werden insbesondere die für die Netzwerksicherheit zentralen Authentisierungs- und Schlüsselaustauschprotokolle eingeführt, welche in Kapitel 8 im Kontext von Gruppenkommunikationsszenarien vertieft werden. Diese vertiefte Diskussion kann in einem einführenden Kurs über das Thema auch weggelassen werden, ohne dass das Verständnis der weiteren Teile des Buches davon beeinflusst würde. Das den ersten Teil beschließende Kapitel 9 gibt eine Einführung in Prinzipien der Zugriffskontrolle.

Teil 2 führt in Architekturen und Protokolle der Netzsicherheit ein.

Der zweite Teil des Buches behandelt Architekturen und Protokolle der *Netzsicherheit*. Kapitel 10 führt zunächst in die allgemeine Fragestellung der Integration von Sicherheitsdiensten in Kommunikationsarchitekturen ein. Kapitel 11 erläutert Sicherheitsprotokolle der Datensicherungsschicht, Kapitel 12 behandelt die Sicherheitsarchitektur für das Internetprotokoll *IPsec* und Kapitel 13 beschreibt Sicherheitsprotokolle der Transportschicht.

Teil 3 ist der drahtlosen und mobilen Kommunikation gewidmet.

Im dritten Teil dieses Buches wird das Gebiet der *sicheren drahtlosen beziehungsweise mobilen Kommunikation* vorgestellt. Kapitel 14 grenzt die bei mobiler Kommunikation zusätzlich auftretenden Sicherheitsaspekte von denen der Festnetze ab und stellt eher konzeptionelle Ansätze zur Wahrung der Vertraulichkeit des aktuellen Aufenthaltsortes mobiler Geräte vor. Die verbleibenden Kapitel dieses Buchteils untersuchen konkrete Systembeispiele. Kapitel 15 behandelt die Sicherheitsfunktionen des Standards *IEEE 802.11* für drahtlose lokale Netze einschließlich der Schwächen früher Versionen dieses Standards. Kapitel 16 führt in die Sicherheitsfunktionen der europäischen Standards für mobile Weitverkehrsnetze *GSM*, *UMTS* und *LTE* ein.

Während die vorhergehenden Teile des Buches sich hauptsächlich auf die Sicherheit von Kommunikationsvorgängen zwischen Endsystemen konzentrieren, geht der vierte und letzte Teil des

Teil 4 beschäftigt sich mit dem Schutz von Kommunikationsinfrastrukturen.

Buches auf die *Sicherung großer Netzwerke und der Kommunikationsinfrastrukur* ein. Kapitel 17 beschreibt dazu zunächst das grundlegende Problem des Schutzes von Systemen in offenen Netzen und gibt eine kurze Übersicht über die systematische Bedrohungsanalyse. Darüber hinaus wird das Problem der Sicherung der Endsysteme als Voraussetzung eines sicheren Netzbetriebs behandelt. Das folgende Kapitel 18 befasst sich mit *Sabotageangriffen*, die Endsysteme und Kommunikationsinfrastruktur gleichermaßen betreffen. Kapitel 19 und Kapitel 20 beschäftigen sich mit der Sicherheit grundlegender Dienste einer Kommunikationsinfrastruktur: dem *Routing* und der *Namensauflösung*. *Internet-Firewalls* als wichtigstes Mittel zur Realisierung einer subnetzbezogenen Zugriffskontrolle werden in Kapitel 21 eingeführt. Da Angriffe nicht immer nur durch die vorgestellten proaktiven Schutzmaßnahmen verhindert werden können, ist oft eine zusätzliche Kontrolle durch *Intrusion-Detection-Systeme* beziehungsweise *Intrusion-Prevention-Systeme* sinnvoll. Deren Grundlagen und existierende Verfahren werden in Kapitel 22 vorgestellt. Das abschließende Kapitel 23 beschäftigt sich mit dem Management großer Sicherheitsinfrastrukturen.

Das Gebiet der Netzsicherheit ist von großer Dynamik geprägt.

An dieser Stelle sei dem Leser vor der weiteren Lektüre des Buches mitgegeben, dass sich das Gebiet der Netzsicherheit in den letzten Jahren als ein sehr aktives Gebiet erwiesen hat, und dass aus diesem Grund ständig eine Vielzahl von Verbesserungen existierender Sicherheitsprotokolle sowie auch neue Protokolle entwickelt und eingeführt werden. Der Schnelligkeit dieser Entwicklung in einem Lehrbuch Rechnung zu tragen, ist daher ein ausgesprochen schwieriges, wenn nicht unmögliches Unterfangen. Aus diesem Grund möge der Leser verzeihen, wenn das eine oder andere Detail zum Zeitpunkt seiner Lektüre bereits auf andere Weise gelöst wird beziehungsweise sich vollständig neue Protokolle etabliert haben, ohne dass sie im vorliegenden Buch behandelt werden. Gerade aufgrund der rasanten Entwicklung des Gebietes wurde als vordringliches Ziel dieses Buches ins Auge gefasst, dem Leser ein grundlegendes Verständnis der jeweils zentralen Prinzipien zu vermitteln und diese anhand konkreter und praxisrelevanter Beispielprotokolle zu erläutern.

1.2 Bedrohungen und Sicherheitsziele

Eine zentrale Rolle bei der Einschätzung von Risiken in Kommunikationsnetzen spielen die Begriffe *Bedrohung* und *Sicherheitsziel*. Sie sollen daher im Folgenden zunächst generisch definiert werden.

Definition 1.1 *Eine* **Bedrohung** *in einem Kommunikationsnetz ist ein potenzielles Ereignis beziehungsweise eine Reihe von Ereignissen, die zur Gefährdung eines oder mehrerer Sicherheitsziele führt. Die tatsächliche Realisierung einer Bedrohung nennt man einen* **Angriff**.

Beispiele für konkrete Bedrohungen

Die oben gegebene Definition 1.1 ist recht abstrakt und greift zudem auf den erst im Folgenden zu definierenden Begriff des Sicherheitsziels zurück. Zur Verdeutlichung können die folgenden Beispiele für Bedrohungen herangezogen werden:

- Ein Angreifer (»Hacker«) dringt in einen Rechner eines Unternehmens ein.
- Mitlesen von übertragenen E-Mails
- Ändern sensibler Kontodaten in einem Abrechnungssystem
- Ein Angreifer legt einen Webserver zeitweise still.
- Jemand nutzt beziehungsweise bestellt Dienstleistungen und Güter im Namen eines anderen.

Beispiele für Sicherheitsziele

Auch der Begriff *Sicherheitsziel* kann zunächst besser anhand einiger Beispiele verstanden werden, da Sicherheitsziele in Abhängigkeit von dem betrachteten Anwendungsszenario auf den ersten Blick sehr unterschiedlich erscheinen:

- Banken:
  - Schutz vor vorsätzlicher oder unbeabsichtigter Modifikation von Transaktionen
  - Zuverlässige und nicht manipulierbare Identifizierung von Kunden
  - Schutz persönlicher Identifikationsnummern vor Offenlegung
  - Schutz persönlicher Kundendaten
- Verwaltung:
  - Schutz vor Offenlegung sensitiver Information
  - Realisierung elektronischer Signaturen für Verwaltungsdokumente
- Öffentliche Netzbetreiber:
  - Beschränkung des Zugriffs auf Managementfunktionen des Netzes nur für autorisierte Betriebskräfte
  - Schutz der Verfügbarkeit angebotener Dienste
  - Gewährleistung einer korrekten und manipulationssicheren Abrechnung von Dienstnutzungen
  - Schutz persönlicher Kundendaten

- Unternehmens- und private Netze:
  - Schutz der Vertraulichkeit von ausgetauschten Daten
  - Sicherstellung der Authentizität von Nachrichten (siehe unten)
- Alle Netze: Schutz vor externen Eindringlingen

Allgemeine Definition von Sicherheitszielen

Einige der oben aufgeführten Sicherheitsziele sind natürlich für mehrere Anwendungsszenarien relevant; wenngleich sie oben nicht mehrfach genannt sind. Sicherheitsziele können aber auch unabhängig von einem konkreten Anwendungsszenario aus rein technischer Sicht definiert werden.

Definition 1.2 *Im Allgemeinen können bei Kommunikationsnetzen die folgenden* **technischen Sicherheitsziele** *unterschieden werden:*

- **Vertraulichkeit (Confidentiality):** *Übertragene oder gespeicherte Daten und/oder spezifische Details eines Kommunikationsvorgangs (zum Beispiel die Identität des Absenders oder Empfängers einer Nachricht) sollen nur berechtigten Instanzen bekannt werden können.*
- **Datenintegrität (Data Integrity):** *Es muss möglich sein, unbeabsichtigte oder vorsätzliche Datenänderungen zu erkennen. Hierfür ist es erforderlich, den Urheber (Erzeuger) von Daten eindeutig und nicht manipulierbar zu identifizieren.*
- **Zurechenbarkeit (Accountability):** *Es muss möglich sein, die für ein bestimmtes Ereignis (zum Beispiel eine Dienstnutzung) verantwortliche Instanz zu identifizieren.*
- **Verfügbarkeit (Availability):** *Die in einem System realisierten Dienste sollen verfügbar sein und korrekt funktionieren.*
- **Kontrollierter Zugang (Controlled Access):** *Nur autorisierte Instanzen sollen auf bestimmte Dienste und Daten zugreifen können.*

Das letzte Ziel wird nicht von allen Sicherheitsexperten als eigenständig angesehen. In Kommunikationsnetzen ist es aber oft durchaus sinnvoll, den Zugang zum Netz zu beschränken, obwohl für das lokale Netz durch einen unautorisierten Zugang keine direkte Bedrohung erwächst.

Allgemeine technische Bedrohungen

Ebenso wie Sicherheitsziele können auch Bedrohungen aus primär technischer Sicht betrachtet werden und somit lassen sich die folgenden *technischen Bedrohungen* unterscheiden:

	Technische Bedrohungen						
Technische Sicherheitsziele	Maskerade	Abhören	Autorisierungsverletzung	Verlust oder Modifikation von Information	Fälschen von Information	Abstreiten von Ereignissen	Sabotage (z.B. durch Überlast)
Vertraulichkeit	x	x	x				
Datenintegrität	x		x	x	x		
Zurechenbarkeit	x		x	x		x	
Verfügbarkeit	x		x	x			x
Kontrollierter Zugriff	x		x		x		

Tabelle 1.1 *Technische Sicherheitsziele und Bedrohungen*

- *Maskerade:* Eine Instanz gibt vor, die Identität einer anderen Instanz zu haben.
- *Abhören:* Eine Instanz liest eine Information, die eigentlich nicht für sie bestimmt ist.
- *Autorisierungsverletzung:* Eine Instanz nutzt Dienste oder Ressourcen, die sie eigentlich nicht nutzen sollte.
- *Verlust oder Modifikation von Information:* Bestimmte Informationen werden zerstört oder modifiziert.
- *Fälschung von Information:* Eine Instanz erzeugt neue Information unter Benutzung der Identität einer anderen Instanz.
- *Abstreiten von Ereignissen:* Eine Instanz gibt fälschlicherweise vor, nicht an einem bestimmten Ereignis beteiligt gewesen zu sein.
- *Sabotage:* Jede Aktion, die zum Ziel hat, die Verfügbarkeit oder korrekte Funktion von Diensten oder Systemen zu reduzieren. Im englischsprachigen Raum werden diese Angriffe mit dem Begriff *Denial-of-Service (DoS)* bezeichnet.

Auf der Grundlage dieser Begriffe ist es möglich, eine allgemeine Zuordnung vorzunehmen, die verdeutlicht, welche Sicherheitsziele primär durch welche Bedrohungen gefährdet werden. Tabelle 1.1 zeigt diese Zuordnung im Überblick. Die Tabelle kann auf zwei Arten gelesen werden: Zum einen zeigt sie zum Beispiel, dass die Vertraulichkeit von Informationen durch die technischen Bedrohungen Maskerade, Abhören und Autorisierungsverletzung gefährdet ist. Zum anderen kann auch direkt abgelesen werden, dass zum Beispiel die Fälschung von Information primär die Sicherheitsziele Datenintegrität, Zurechenbarkeit und kontrollierter Zugang gefährdet.

Reale Angriffe kombinieren oft mehrere Bedrohungen.

In der Realität werden die oben genannten Bedrohungen oft kombiniert, um einen konkreten Angriff zu realisieren. So wird das Eindringen in ein System häufig dadurch realisiert, dass zunächst eine Zugangskennung und das dazugehörende Passwort abgehört werden und dann die Identität der abgehörten Kennung bei der Zugangsprüfung vorgegeben wird, wobei Letzteres eine Maskerade darstellt. Aus diesem Grund dient Tabelle 1.1 eher erläuternden Zwecken, als dass sie konkrete Fähigkeiten oder Möglichkeiten unterschiedlicher Angreifer definiert.

1.3 Sicherheitsanalyse für Netze

Szenarienbezogene Bewertung von Bedrohungen

Um geeignete Maßnahmen gegen die oben genannten Bedrohungen in einem konkreten Anwendungsszenario treffen zu können, müssen diese zunächst sorgfältig für die in dem Szenario verwendete Netzwerkkonfiguration bewertet werden. Dies erfordert eine detaillierte *Sicherheitsanalyse* der eingesetzten Netztechnologie, die das Risikopotenzial der technischen Bedrohungen für die in einem Netz kommunizierenden Instanzen evaluiert und hierbei auch den Aufwand im Sinne erforderlicher Ressourcen (Rechenkapazität, Speicher, Nachrichtenübermittlung) für die Ausführung bekannter Angriffstechniken bewertet.

Achtung: Es ist nicht möglich, unbekannte Angriffstechniken zu bewerten!

Eine solche detaillierte Sicherheitsanalyse für eine gegebene Netzkonfiguration beziehungsweise eine spezifische Protokollarchitektur kann unter Umständen auch nötig sein, um das finanzielle Controlling eines Unternehmens von der Notwendigkeit erforderlicher Sicherheitsmaßnahmen zu überzeugen. Da sowohl die Angriffstechniken als auch die Netzwerkkonfigurationen in der Regel einem ständigen Wandel unterworfen sind, muss das Risiko oft sogar fortlaufend bewertet werden. Bei großen Unternehmen bietet es sich hierzu an, ein Sicherheitsmanagement nach ISO 27001 [ISO13] umzusetzen, indem etwa eine Stelle für einen dedizierten Sicherheitsbeauftragten geschaffen wird.

Eine Schlüsselfrage in Bezug auf durchzuführende Sicherheitsanalysen ist in jedem Fall, wie die Komplexität des Gesamtsystems reduziert werden kann. Einige grundlegenden Techniken werden hierzu in Kapitel 17 vertiefend betrachtet werden, aber eine Sicherheitsanalyse für eine spezifische Protokollarchitektur kann etwa gemäß den folgenden, feingranularen *Angriffen auf Nachrichtenebene* strukturiert werden:

- Passive Angriffe: Abhören von Protokolldateneinheiten (Protocol Data Units, PDUs)
- Aktive Angriffe: Verzögern, Wiedereinspielen, Löschen, Modifizieren und Einfügen von PDUs

Kombination von Angriffen

Bei jeglicher Sicherheitsanalyse sollte in jedem Fall davon ausgegangen werden, dass ein realer Angreifer die oben genannten Angriffe miteinander kombinieren können muss, um komplexere Angriffe zusammensetzen zu können. Es handelt sich also um als Angriffsprimitive zu verstehende Grundbausteine. Von einem »erfolgreichen Angriff« auf Nachrichtenebene werden daher die folgenden Eigenschaften gefordert, da sonst gegebenenfalls keine komplexeren Angriffe ausgeführt werden können, weil der Angriff etwa entdeckt wird und Gegenmaßnahmen eingeleitet werden:

- Der Angriff erzeugt keine direkt erkennbaren Nebeneffekte für andere Kommunikationsvorgänge, zum Beispiel für andere Verbindungen oder verbindungslose Datenübertragungen.
- Der Angriff erzeugt kaum Nebeneffekte für andere PDUs der gleichen Verbindung beziehungsweise der verbindungslosen Datenübertragung zwischen den an der Kommunikation beteiligten Instanzen.

Bei der Sicherheitsanalyse einer Protokollarchitektur sind die oben genannten Angriffe für jede einzelne Schicht der Architektur zu untersuchen.

Gliederung von Protokollfunktionen in fünf Schichten

Abbildung 1.1 zeigt die heutzutage übliche Architektur geschichteter Kommunikationssysteme. In dieser kommunizieren Endsysteme über ein Netz von Zwischensystemen miteinander. Die hierfür erforderlichen Protokollfunktionen werden in fünf Schichten organisiert:

- Die unterste Schicht ist die *Bitübertragungsschicht*. Sie realisiert die Übertragung eines Bitstroms über ein physikalisches Medium (zum Beispiel eine Leitung oder eine Funkübertragungsstrecke).
- Die darüber liegende *Datensicherungsschicht* fasst mehrere Bits aus dem zu übertragenden Bitstrom zu Übertragungsrahmen zusammen und realisiert eine gegen Fehler gesicherte Übertragung zwischen zwei über ein physikalisches Medium verbundenen Systemen. In diesem Zusammenhang erfüllt sie zwei grundsätzliche Aufgaben: Im Fall eines Übertragungsmediums, welches mehreren Systemen gemeinsam zur Verfügung steht, steuert sie den Zugriff *(Medium Access Control,*

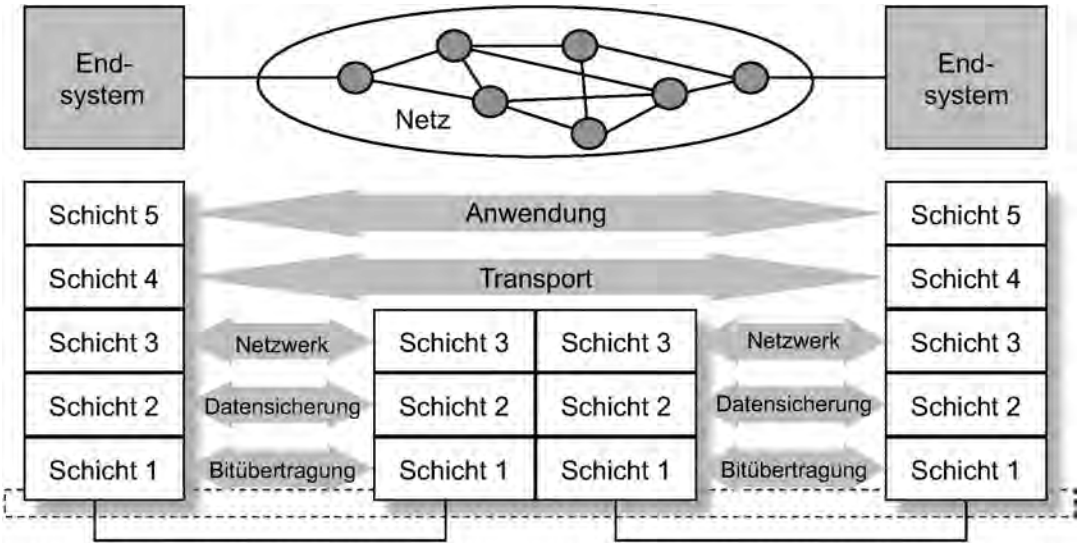

Abbildung 1.1 *Architektur geschichteter Kommunikationssysteme*

MAC). Darüber hinaus trifft sie Maßnahmen zur Erkennung von Übertragungsfehlern, sodass fehlerhaft empfangene Rahmen beim Empfänger erkannt und verworfen werden können.

- Die *Netzwerkschicht* realisiert die Kommunikation zwischen Endsystemen, die in der Regel über mehrere Zwischensysteme miteinander verbunden sind. Eine zentrale Aufgabe dieser Schicht ist somit die Wahl des Weges (Routing) durch das Vermittlungsnetz zwischen den beiden Endsystemen.
- Die *Transportschicht* ermöglicht den Austausch von Daten zwischen den Prozessen der Endsysteme. Die wesentlichen Aufgaben dieser Schicht sind die Adressierung von Anwendungsprozessen, die Fehlererkennung auf Ende-zu-Ende-Ebene und im Fall eines zuverlässigen Dienstes auch Maßnahmen zur Fehlerbehebung (zum Beispiel durch Übertragungswiederholung).
- Oberhalb der Transportschicht realisiert die *Anwendungsschicht* – wie ihr Name nahelegt – anwendungsspezifische Protokolle, die so vielfältig sind, wie die in den Endsystemen ablaufenden Anwendungen.

In den (Zwischen-)Systemen des Vermittlungsnetzes werden in der Regel lediglich die unteren drei Schichten bis zur Netzwerkschicht implementiert.

Gliederung der Sicherheitsanalyse

Die Sicherheitsanalyse geschichteter Protokollarchitekturen kann gemäß der oben gegebenen Beschreibung entlang zweier

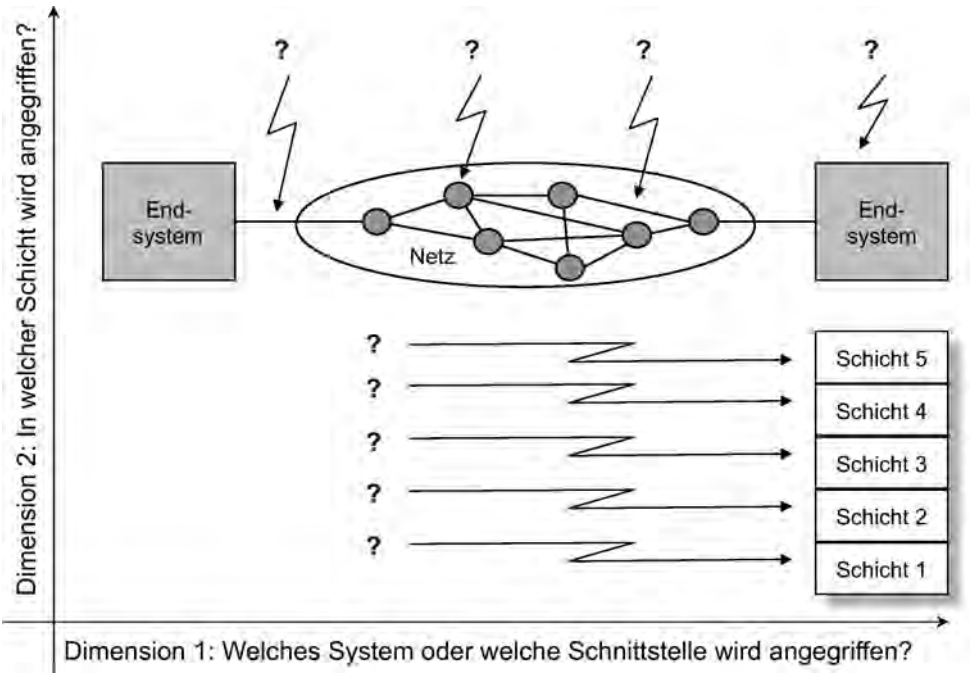

Abbildung 1.2 *Dimensionen der Sicherheitsanalyse geschichteter Protokollarchitekturen*

Dimensionen gegliedert werden (vergleiche hierzu auch Abbildung 1.2):

- Zunächst müssen innerhalb der zu untersuchende Netzkonfiguration *gefährdete Systeme und Schnittstellen* identifiziert werden. Besondere Gefährdungen ergeben sich beispielsweise aus öffentlich zugänglichen Endsystemen, an Übergängen zu öffentlichen Netzen, aber auch durch nicht gesicherte Übertragungsstrecken (insbesondere bei drahtloser Übertragung).
- Weiterhin wird die Sicherheitsanalyse danach gegliedert, *in welcher Schicht* ein Angriff erfolgen kann. Angriffe müssen nicht notwendigerweise in der Anwendungsschicht erfolgen, im Gegenteil, je nach Intention des Angreifers können sogar hauptsächlich die Schichten unterhalb der Transportschicht den Hauptangriffspunkt darstellen.

Eine detaillierte Sicherheitsanalyse ist bei der Identifizierung der in einer bestimmten Netzkonfiguration vorherrschenden Sicherheitsrisiken sehr nützlich. Auf ihrer Grundlage können im Anschluss geeignete Sicherheitsmaßnahmen zur Reduzierung der Risiken ausgewählt werden. Einen allgemeinen Überblick hierüber liefert der folgende Abschnitt.

1.4 Maßnahmen der Informationssicherheit

Es gibt eine Vielzahl unterschiedlicher Sicherheitsmaßnahmen, die jeweils bestimmte Aspekte eines informationsverarbeitenden Systems und seiner Einbettung in die durch das System zu unterstützenden Arbeitsabläufe aufgreifen:

- *Physikalische Sicherheitsmaßnahmen* umfassen Schließsysteme und physikalische Zugangskontrollen, die manipulationssichere Gestaltung (»Tamper-Proofing«) sicherheitssensitiver Geräte sowie umgebungsüberwachende Kontrollen, wie zum Beispiel Bewegungsmelder.
- *Personelle Sicherheitsmaßnahmen* beginnen mit der Einstufung der sicherheitsspezifischen Sensitivität einer Position und umfassen weiterhin Abläufe zur Überprüfung des Personals sowie Schulungs- und Sensibilisierungsmaßnahmen in Bezug auf sicherheitsrelevante Aspekte.
- *Administrative Sicherheitsmaßnahmen* umfassen Prozeduren für die kontrollierte Einbringung neuer Software und Hardware, die Erkennung sicherheitsrelevanter Vorkommnisse durch das Führen und regelmäßige Überprüfen von Ereignisprotokollen sowie die Untersuchung erkannter sicherheitsrelevanter Verstöße und Vorkommnisse.
- *Maßnahmen der Mediensicherheit* zielen auf die Sicherung der Speicherung von Informationen ab. Hierzu werden Abläufe und Kontrollmechanismen für die Kennzeichnung, Reproduktion und Zerstörung sensitiver Informationen und Datenträger implementiert.
- Vorkehrungen der *Abstrahlungssicherheit* verhindern beziehungsweise begrenzen elektromagnetische Emissionen von Rechensystemen und Peripheriegeräten (insbesondere Monitore), die von einem Angreifer sonst aufgezeichnet und zum Abhören von Informationen verwendet werden können.
- *Kontrollen des Entwicklungszyklus von Systemen* überwachen den Entwurf, die Implementierung und die Einführung informationsverarbeitender Systeme. Hierbei wird durch die Vorgabe und Kontrolle einzuhaltender Standards der Programmierung und der Dokumentation ein »vertrauenswürdiger« Entwicklungsprozess angestrebt.
- Maßnahmen der *Systemsicherheit* von Computern, Betriebssystemen und den auf den Computern ausgeführten Anwen-

dungen haben zum Ziel, die in Rechensystemen gespeicherten und verarbeiteten Informationen zu sichern.

- In Ergänzung zu der letztgenannten Kategorie zielen Maßnahmen der *Kommunikationssicherheit* darauf ab, Informationen während ihrer Übermittlung in einem Kommunikationsnetz zu schützen. Zusammen mit Vorkehrungen zum Schutz der Netzinfrastruktur selbst bilden sie die Maßnahmenkategorie der *Netzsicherheit*.

Die sichere Gestaltung eines Informationsverarbeitungsprozesses erfordert eine umfassende Anwendung des Maßnahmenkatalogs.

Den Hauptgegenstand des vorliegenden Buches bildet die letztgenannte Kategorie, die Netzsicherheit. An dieser Stelle sei jedoch ausdrücklich darauf hingewiesen, dass zur Gewährleistung sicherer Informationsverarbeitungsprozesse eine sorgfältige Anwendung des gesamten oben aufgeführten Maßnahmenkatalogs erforderlich ist. Das ist durch die Tatsache begründet, dass ein Sicherheitssystem nur so sicher ist wie seine schwächste Komponente. Der Einsatz eines technisch ausgereiften Passwortsystems, das die Verwendung leicht zu erratender Passwörter verhindert, ist beispielsweise von geringer Effektivität, wenn Benutzer ihre Passwörter auf nicht ausreichend geschützte Medien schreiben oder von einem Angreifer per Anruf dazu gebracht werden können, sie zu verraten (»Social Engineering«).

1.5 Zentrale Begriffe der Kommunikationssicherheit

In diesem Abschnitt werden die für die Netzsicherheit zentralen Begriffe *Sicherheitsdienst, kryptografischer Algorithmus* und *kryptografisches Protokoll* eingeführt und ihre Beziehungen untereinander erläutert.

Definition 1.3 *Ein* **Sicherheitsdienst** *ist ein abstrakter Dienst, der zur Erreichung eines bestimmten Sicherheitsziels realisiert wird.*

Realisierung von Sicherheitsdiensten

Ein Sicherheitsdienst kann sowohl mit kryptografischen als auch mit herkömmlichen Mitteln realisiert werden. So kann beispielsweise das unberechtigte Auslesen einer auf einem USB-Stick gespeicherten Datei zum einen dadurch verhindert werden, dass die Datei vor der Speicherung verschlüsselt wird. Zum anderen wird das gleiche Ziel aber auch durch das Wegschließen des USB-Sticks in einem sicheren Safe erreicht. In der Regel ist eine Kombination kryptografischer und herkömmlicher Methoden am effektivsten.

Fundamentale Sicherheitsdienste

Die oben gegebene Definition 1.3 legt in ihrer Allgemeinheit den Schluss nahe, dass eine Vielzahl unterschiedlicher Sicherheitsdienste existiert. Tatsächlich ist die Zahl der gemeinhin unterschiedenen Sicherheitsdienste aber erstaunlich gering; genau fünf fundamentale Sicherheitsdienste werden differenziert:

- Die *Authentisierung (Authentication)* stellt, wie sich im weiteren Verlauf dieses Buches noch zeigen wird, den wichtigsten Sicherheitsdienst dar, da sie die manipulationssichere Identifikation von Instanzen ermöglicht.
- Der Sicherheitsdienst *Datenintegrität (Data Integrity)* ist in gewisser Hinsicht »der kleine Bruder« des Authentisierungsdienstes, da er sicherstellt, dass von einer bestimmten Instanz erzeugte Daten nicht unbemerkt modifiziert werden können.
- Die *Vertraulichkeit (Confidentiality)* ist der wohl bekannteste Sicherheitsdienst, der verhindern soll, dass Informationen unautorisierten Instanzen bekannt werden.
- Der Sicherheitsdienst *Zugriffskontrolle (Access Control)* überwacht, dass lediglich jene Instanzen, die dazu berechtigt sind, in festgelegter Weise auf bestimmte Informationen und Dienste zugreifen können.
- Das Ziel des Dienstes *Urhebernachweis (Non-Repudiation)* ist es, die Urheber von bestimmten Aktionen, zum Beispiel dem Senden einer Nachricht, eindeutig identifizieren zu können, sodass diese getätigte Aktionen im Nachhinein nicht abstreiten können. Im Gegensatz zur Authentisierung ist dieser Nachweis gegenüber Dritten möglich.

Definition 1.4 *Ein* **kryptografischer Algorithmus** *ist eine mathematische Abbildung von Eingabedaten (zum Beispiel Daten und Schlüssel) auf Ausgabedaten.*

Kryptografische Algorithmen spielen eine wichtige Rolle bei der Realisierung von Sicherheitsdiensten. Die Verwendung eines kryptografischen Algorithmus alleine ist jedoch nicht ausreichend hierfür, da zusätzlich noch die Einbettung des Algorithmus in einen semantischen Kontext erforderlich ist. Diese erfolgt in der Regel im Rahmen der Definition eines *kryptografischen Protokolls*.

Definition 1.5 *Ein* **kryptografisches Protokoll** *ist eine Ablaufvorschrift für eine Reihe von Verarbeitungsschritten und zwischen mehreren Instanzen auszutauschenden Nachrichten, mit deren Ausführung ein bestimmtes Sicherheitsziel erreicht werden soll.*

Die beiden zuletzt definierten Begriffe der kryptografischen Algorithmen und Protokolle sind von so grundlegender Bedeutung für die Netzsicherheit, dass sie in diesem Buch in mehreren Kapiteln behandelt werden. Bevor jedoch konkrete Algorithmen und Protokolle vorgestellt werden sollen, werden im nächsten Kapitel zuvor allgemeine Grundlagen der Kryptologie eingeführt.