STUDIENSKRIPT



## Netzwerksicherheit

DLMCSEESN01\_E



Übergeordnete Lernziele

##### Einführung 9



Die Informationstechnologie (IT) ist in vielen realen Umfeldern und unterschiedlichen Wirtschaftszweigen von entscheidender Bedeutung. Hierzu gehören unter anderem auch Gesund­heit, Mobilität, Unterhaltung, Fertigung, Logistik und Finanzen. Eine sichere IT-Infrastruktur ist für Innovationen unerlässlich. IT-Sicherheit verhindert Wirtschaftsspionage, wirtschaftliche Schäden durch Hackerangriffe und körperliche Schäden durch manipulierte oder unzuverlässige eingebettete Systeme.

Fundierte Kenntnisse über den Schutz und die Zuverlässigkeit von Netzwerkinfrastrukturen spielen eine entscheidende Rolle bei der Entwicklung und Implementierung von IT-Systemen. Der Kurs Netzwerksicherheit vermittelt den nötigen Hintergrund zum Verständnis sicherer Netzwerktechnik. Der Kurs führt in die Grundlagen der Computernetzwerke ein und hat dabei die folgenden Schwerpunkte: Die Internetprotokollfamilie (TCP/IP), die Sicherung der Netzwerkinfrastruktur, das Verständnis von Netzwerksicherheitsproblemen und ‑bedrohungen, die Überprüfung auf Schwachstellen in der Netzwerksicherheit sowie die Vorstellung verschiedener Sicherheitsmechanismen zur Abwehr von Angriffen und Identifikation von Schwachstellen. Die Kenntnis dieser Mechanismen ist für den Entwurf und die Implementierung von Netzwerksicherheitsstrategien unerlässlich.

Nach Abschluss dieses Kurses verstehen die Studierenden, wie man verschiedene Systeme in einer vernetzten Umgebung absichert, wie man Systemsicherheit bewertet und wie man Sicherheitsanforderungen und Abhilfemaßnahmen ermittelt. Der Kurs vermittelt ein Verständnis dafür, wie Geräte der Infrastruktur und die Kommunikation zwischen Computersystemen gesichert werden können. Darüber hinaus werden Sie mit einer Reihe von Strategien vertraut gemacht, darunter kryptografische Techniken, Cloud-Sicherheit sowie Mechanismen zur Erkennung von Angriffen und wie man diese verhindern kann.



# Lektion 1

## Netzwerksicherheit im Überblick

#### LERNZIELE

Nach Abschluss dieser Lektion werden Sie in der Lage sein, …

… die Grundlagen von Computernetzwerken zu verstehen, insbesondere die Internet-Protokollfamilie (TCP/IP).

… die Konzepte der passiven und aktiven Erfassung des Netzwerkverkehrs zu identifizieren.

… übliche Schwachstellen in der Netzwerksicherheit zu erkennen.

… Informationen zu den technischen Aspekten der Sicherung von Netzwerkprotokollen anzuwenden.

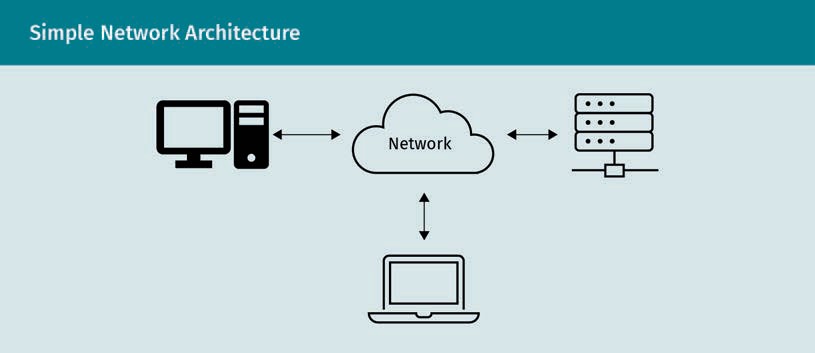
DL-E-DLMCSEESN01\_E-U01

1. Netzwerksicherheit im Überblick

### Einführung

Ein Netzwerk ist eine Gruppe von Geräten (Computern), die miteinander verbunden sind und Informationen austauschen. Jedes angeschlossene Gerät wird als Knoten im Netzwerk bezeichnet, was die Bezeichnung auf eine breite Palette unterschiedlicher Geräte verallgemeinert. Die folgende Abbildung zeigt ein Beispiel für ein einfaches Netzwerk mit drei Knoten, die an ein gemeinsames Netzwerk angeschlossen sind. Jeder Knoten kann mit unterschiedlicher Software oder Hardware ausgestattet sein. Daher muss jeder Knoten eine Reihe von Regeln befolgen, um mit den anderen Knoten im Netzwerk zu kommunizieren.

Die Kanten (Linien) zwischen den Knoten modellieren die Verbindungen zwischen den kommunizierenden Geräten. Das Netzwerk umfasst zwei verschiedene Arten von Topologien, eine physische und eine logische. Die physische Topologie beschreibt, wie die verschiedenen Komponenten im Netzwerk platziert sind (z. B. die Position der Geräte und die Verlegung der Kabel). Die logische Topologie hingegen gibt an, wie die Daten im Netzwerk fließen.



### Grundlegende Protokollschichtung

Bevor wir die Definition eines Netzwerkprotokolls erläutern, betrachten wir ein Beispiel, das die Kommunikation zwischen zwei Parteien zeigt. Stellen Sie sich zwei Professoren vor, von denen einer Englisch und der andere Chinesisch und Französisch spricht, wie in der nachstehenden Abbildung dargestellt (Tanenbaum & Wetherall, 2010). Da sie keine gemeinsame Sprache sprechen, nehmen sie einen Übersetzer hinzu, der dann eine Sekretärin bittet, die übersetzte Nachricht zu versenden. Der Professor gibt also eine Nachricht (auf Englisch) an seinen Übersetzer weiter, in der es heißt: „The deadline is on 1/5/2021“. Die Übersetzer haben sich darauf geeinigt, eine neutrale Sprache zu verwenden, die beide kennen, nämlich Deutsch. Die Meldung wird also in *„Einsendeschluss ist am 1.5.2021“* umgewandelt. Anschließend gibt der Übersetzer die Nachricht an die Sekretärin zur Übermittlung per E-Mail weiter. Nachdem die Nachricht bei der anderen Sekretärin angekommen ist, gibt diese sie an den Übersetzer vor Ort weiter. Dieser übersetzt sie ins Französische und leitet sie an den zweiten Professor weiter.

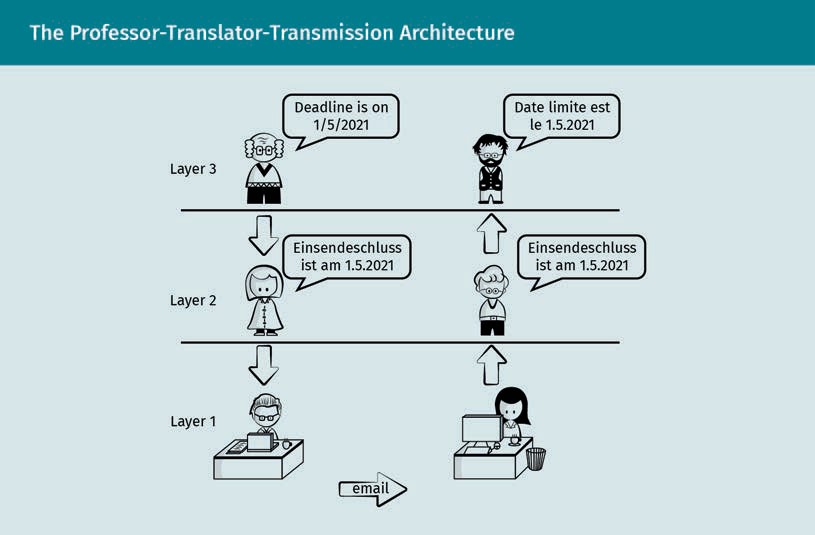
Anhand dieses Beispiels können wir die folgenden Begriffe definieren. Wenn das Modell als übereinander liegende Schichten oder Ebenen organisiert wird, lässt sich die Komplexität des Professor-Beispiels verringern. Jede Schicht baut auf der darunter liegenden auf. Die Professoren befinden sich beispielsweise auf Ebene (Schicht) drei, und beide kontaktieren ihre Übersetzer auf der darunter liegenden Ebene (Ebene bzw. Schicht zwei). Die Übersetzer kommunizieren dann mit den Sekretärinnen in der ersten Ebene (Schicht). Die Parteien jeweils einer Schicht werden Peers *(engl. Gleichgestellte, Ebenbürtige)* genannt. Die Peers können Geräte (Hardware), Menschen oder Software-Prozesse sein.

Die Peers verwenden **Protokolle**, um miteinander zu kommunizieren. Zum Beispiel haben sich die beiden Übersetzer auf die Nutzung des Deutschen geeinigt. Mit anderen Worten: Sie haben sich für eine Kommunikationssprache entschieden. Außerdem haben sich die beiden Sekretärinnen für die Übermittlung per E-Mail entschieden. Manchmal kann ein Protokoll auf einer bestimmten Schicht geändert werden, ohne dass dies die angrenzenden oder benachbarten Schichten beeinträchtigt. Anders gesagt: Weder die darüber noch die darunter liegenden Schichten merken etwas davon. In unserem Beispiel können die Sekretärinnen ihre Kommunikation von E-Mail auf Fax umstellen, ohne die anderen Ebenen (Schichten) zu informieren. Schließlich findet zwischen zwei benachbarten Schichten ein Austausch statt. Mit anderen Worten: Es gibt eine Schnittstelle zwischen jeweils zwei Ebenen (Schichten). Die Schnittstelle definiert die Dienste und Vorgänge (Operationen), welche die untere Schicht an die obere liefert. In Wirklichkeit werden gar keine Daten direkt von Professor eins auf Professor zwei übermittelt. Stattdessen leitet jede Schicht Daten nach unten weiter, bis die unterste Schicht (d. h. die Sekretärin) erreicht ist. Hier findet die eigentliche Kommunikation statt, wie in der nachfolgenden Abbildung dargestellt.

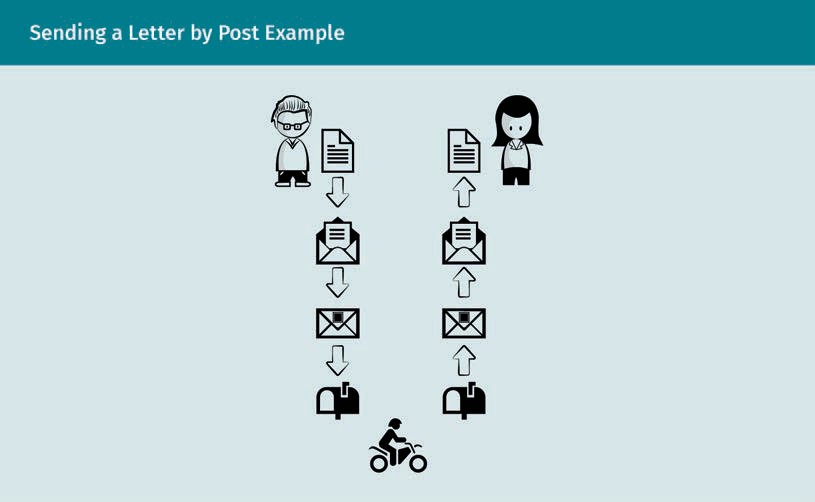
Der Inhalt der einzelnen Schichten und die Anzahl der Schichten variieren möglicherweise von einem Netzwerk zum anderen. Die Aufgabe jeder Schicht ist es, den höheren Schichten spezifische Dienste anzubieten. Zugleich bleiben die Einzelheiten der Implementierung der angebotenen Dienste vor der höheren Schicht verborgen (Abstraktion). Abstraktion bedeutet also, dass eine Software (oder Hardware) den erforderlichen Dienst bereitstellt, ohne deren Details wie Algorithmen oder interne Architektur offenzulegen (Tanenbaum & Wetherall, 2010).

**Protokoll**

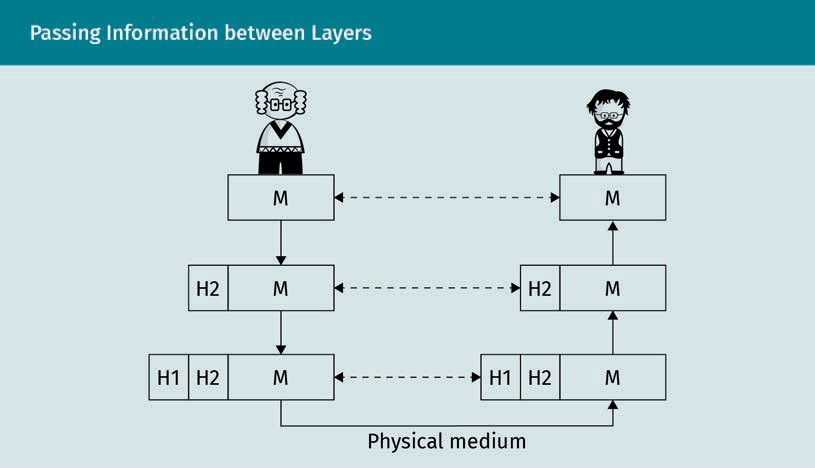
Eine Vereinbarung zwischen den Parteien darüber, wie die Kommunikation ablaufen soll.



Nachdem wir uns auf die grundlegenden Begriffe (Terminologie) geeinigt haben, wollen wir ein weiteres Beispiel betrachten: den Versand eines Briefes per Post, wie in der folgenden Abbildung dargestellt. Der Absender muss den Brief schreiben, ihn in einen Umschlag stecken und schließlich den Namen und die Adresse des Empfängers darauf notieren, bevor er den Umschlag in die Post gibt. Der Name und die Adresse werden als „Header“ (englisch für Kopfzeile oder Vorspann) bezeichnet Auf der anderen Seite erhält der Empfänger später die Post, öffnet den Umschlag und liest den Brief. So können in jedem Schritt (bzw. auf jeder Schicht) bestimmte Informationen (jeweils „Header“ genannt) hinzugefügt werden, bevor die Nachricht an die nächste Schicht weitergegeben wird. Diese Header sind nur für die Peer-Schicht auf der Empfängerseite bestimmt. Einerseits interessiert sich der Postbote nicht für die Daten im Umschlag, sondern nur für die Adresse. Andererseits interessiert sich der Empfänger nur für den Brief und seinen Inhalt, nicht aber für den Umschlag. Die Akteure jeder Schicht fügen dem Brief also jeweils einen Header hinzu, wie zum Beispiel Versiegeln des Briefs, Aufschrift der Adresse usw. Die jeweils entsprechende Schicht auf der Empfängerseite entfernt diesen Header (Kopfzeile) des Briefes und kommt so zur eigentlichen Information dieser Schicht.



Betrachten wir nun ein eher technisches Beispiel mit einem dreischichtigen Netzwerk, wie in der folgenden Abbildung dargestellt. Nehmen wir an, dass jede Schicht virtuell mit der entsprechenden Schicht kommuniziert, wie durch die gestrichelten Linien gezeigt (d. h. Professor eins mit Professor zwei). In Wirklichkeit leitet jedoch jede Schicht Steuerungs- und Inhaltsdaten direkt an die darunter liegende weiter, bis die unterste Schicht (Schicht eins) erreicht ist. Schicht eins beschreibt das physische Medium, über das die eigentliche Kommunikation erfolgt, wie in der Abbildung mit durchgezogenen Linien dargestellt. Eine Nachricht M wird von einem Prozess in der dritten Schicht erstellt und zur Übertragung an die zweite Schicht gesendet. Ein Prozess in Schicht zwei fügt der Nachricht die Steuerungsinformationen (z. B. die Adresse des Zielrechners) hinzu und leitet das Ergebnis an Schicht eins zur physischen Übertragung weiter. Diese Steuerungsinformationen im „Header“ werden der Nachricht vorangestellt, damit die Schicht eins die Nachricht an den Zielcomputer übermitteln kann, wie in der folgenden Abbildung dargestellt. Auf dem Zielrechner wandert die Nachricht von Schicht zu Schicht nach oben, wobei die Header (Kopfzeilen) unterwegs entfernt werden. Es stellen sich jedoch folgende Fragen: Wie viele Schichten werden in einem Netzwerk benötigt, und welche Art von Informationen sollen zwischen den Schichten weitergegeben werden?



In der Regel einigen sich die Netzwerkdesigner auf die Anzahl der Schichten, die in einem Netzwerk enthalten sein sollen, was von der Verwendung der einzelnen Schichten abhängt. Mit anderen Worten: Jede Schicht sollte bestimmte Funktionen erfüllen. Darüber hinaus versuchen Netzwerkdesigner, die zwischen den Schichten weiterzugebende Datenmenge klein zu halten. Dadurch wird es einfacher, eine Schicht durch ein völlig anderes Protokoll oder eine andere Implementierung zu ersetzen. Mit Hilfe der von den Netzwerkdesignern angegebenen Informationen werden die Anzahl der erforderlichen Schichten und die entsprechenden Protokolle ermittelt. Dies wird als Netzwerkarchitektur bezeichnet (Tanenbaum & Wetherall, 2010).

### Das TCP/IP-Referenzmodell

TCP/IP ist heute faktisch das Standardprotokoll, wie es von modernen Netzwerken genutzt wird. Im TCP/IP-Protokoll werden zwei Hauptprotokolle kombiniert: das Internetprotokoll (IP) und ein Protokoll zur Übertragungssteuerung namens *Transmission Control Protocol* (TCP). TCP/IP unterteilt die Netzwerkkommunikation in vier Schichten, wie in der nachstehenden Abbildung dargestellt (Forshaw, 2017).