2 Kommunikation in Netzwerken

Historisch ist nicht abschließend geklärt, wie sich riesige Netzwerke, Dienste und Angebote zu dem entwickelten, was heute oft als *Internet* bezeichnet wird. »Das Internet ist (…) eine komplexe Systementwicklung, die in mehreren Stufen an den Nahtstellen von universitärer und militärischer Großforschung sowie informatischen User-Kulturen entstanden ist« [HELLIGE, 2006, S. 3]. Es kann daher keine zielgerichtete und methodisch strukturierte Entwicklung von kleinen Anfängen bis zum komplexen Endprodukt angegeben werden. Lehrbücher (vgl. [TANENBAUM, 2003; STEIN, 2008; COMER und DROMS, 2002]) gehen typischerweise von einer zielgerichteten Erkenntnisgewinnung aus, um die komplexe Wirklichkeit für den Lernenden in fachlich einfache bzw. grundlegende Konzepte oder Ideen aufzuschlüsseln. Allerdings werden durch die Auswahl konkreter, technischer Problemstellungen bzw. Zielsetzungen Lerngegenstände fokussiert und oft in einen historischen Zusammenhang gesetzt. Z. B. beschreibt TANENBAUM ausführlich die physikalischen Spezifikationen der unterschiedlichsten Netzwerke, etwa Telefon, Kabelfernsehen, Satellitennetzwerke (vgl. [TANENBAUM, 2003, Kap. 2]).

Sicherlich hat ein solcher fachsystematischer Zugang gerade im Bereich der Forschung und Entwicklung seine Berechtigung. Allerdings liegt der Schwerpunkt dieser Arbeit auf der Untersuchung der Auswirkungen einer Interaktion zwischen Mensch und Maschine innerhalb der Situation Cyber-Mobbing. Es ist demnach nicht notwendig, technologisch nachvollziehen zu können, warum bestimmte Techniken entwickelt wurden, sondern die für ein Verständnis der zugrunde liegenden Konzepte notwendigen Kompetenzen sollen identifiziert werden. Dafür werden zunächst die fachlichen Konzepte analysiert und herausgestellt.

A. Hilbig, *Kompetenzen in der Informatik zur Prävention von Cybermobbing*,
BestMasters, DOI 10.1007/978-3-658-14379-4_2

2.1 Kommunikation

Unter Kommunikation wird im Rahmen der fachlichen Analyse der Austausch von digitalen Daten zwischen Maschinen bzw. Informatiksystemen verstanden. Die Schnittstelle zwischen Mensch und Maschine wird in der technischen Realisierung von Kommunikationsprozessen ausgeblendet. Die für die Übertragung wichtigen Referenzmodelle (z. B. OSI, TCP/IP, vgl. [TANENBAUM, 2003, S. 37ff]) modellieren die Übertragung von Daten zwischen Informatiksystemen. Die Referenzmodelle sind in Schichten aufgeteilt. Jede Schicht repräsentiert wichtige Aspekte der Übertragung, etwa die physikalischen Voraussetzungen oder die Anforderungen der einzelnen konkreten Anwendungsprotokolle (z. B. HTTP). Dass möglicherweise konkrete Menschen durch Informatiksysteme kommunizieren könnten, findet keine direkte Berücksichtigung innerhalb der technischen Realisierung.

2.2 Netzwerk

Auch in anderen Wissenschaften sind Netzwerke bekannt, etwa in den Sozialwissenschaften, um die Beziehungen von Menschen zueinander zu untersuchen (vgl. [CHRISTAKIS, FOWLER und NEUBAUER, 2011]). Sofern nicht anders angegeben, wird innerhalb dieser Arbeit der Begriff Netzwerk, wie in diesem Abschnitt definiert, verwendet.

Im Prinzip ist ein Netzwerk (kurz auch Netz genannt) ein Zusammenschluss mehrerer Informatiksysteme, so dass diese untereinander kommunizieren können. Jedes Informatiksystem innerhalb des Netzwerks ist für sich autonom und besitzt eine Verbindung zu mindestens einem weiteren. Zwischen zwei Systemen besteht genau dann eine Verbindung, wenn sie miteinander Daten austauschen können (vgl. [TANENBAUM, 2003, S. 2f]). Es ist unbedeutend, auf welche physikalische Art, z. B. Kupferdraht, Glasfasern, infrarote oder elektromagnetische Wellen, die Systeme verbunden sind, so lange der Austausch von digitalen Daten möglich ist (vgl. [STEIN, 2008, S. 20]).

Innerhalb eines Netzwerks werden die einzelnen Informatiksysteme als Knoten bezeichnet. Zwei Knoten müssen nicht direkt verbunden sein, um miteinander kommunizieren zu können. Die Daten der Kommunikation

können auch über *Zwischensysteme* (vgl. [ebd., S. 20]) weitergeleitet werden. Für die beiden kommunizierenden Knoten, die dann auch als Endknoten bezeichnet werden, entsteht jedoch die Illusion bzw. Abstraktion, sie wären direkt miteinander verbunden. In bestimmten Kontexten bietet einer der Endknoten einen konkreten Nutzen bzw. Dienst an (z. B. eine Webseite, die als Ergebnis auf eine Anfrage ausgeliefert wird). Dann werden die Endknoten erweiternd als Client (Nutzer) und Server (Anbieter) bezeichnet (Client-Server-Prinzip).

2.3 Internet

Das kabelgebundene Telefonnetz ist ein eigenes geschlossenes Netzwerk. Jeder Teilnehmer bzw. jedes Telefon ist ein Endknoten. Das Mobilfunknetz stellt ein davon unabhängiges, eigenes Netzwerk, in dem Mobiltelefone als Endknoten fungieren, dar. Sofern von einem Mobiltelefon ein Festnetztelefon angerufen wird, muss eine Verbindung von einem Knoten aus dem einen Netz zu einem Knoten im anderen hergestellt werden. Dazu muss eine Verbindung zwischen den beiden Netzen vorhanden sein. Für die Endknoten entsteht die Illusion, sie würden direkt miteinander kommunizieren. Aus ihrer Sicht befinden sie sich beide innerhalb des selben logischen Netzwerks. Ein Verbund von verschiedenen sogenannten Subnetzen oder Teilnetzen wird als ein Internet bzw. Internetzwerk bezeichnet (vgl. [ebd., S. 41]).

Der Begriff *Internet* wird im heutigen Sprachgebrauch oftmals nicht eindeutig verwendet. Jedes Internet stellt eine Abstraktion oder *virtuelles Netzwerk* dar (vgl. [ebd., S. 41]). Im Alltag ist mit *dem Internet* typischerweise ein globales Internetzwerk gemeint, dass es unabhängig davon, in welchem Teilnetzwerk sich die Endknoten (geographisch) befinden, ermöglicht, beliebige Dienste und Anwendungen abzurufen bzw. Daten auszutauschen.

Um im weiteren Verlauf Missverständnisse zu vermeiden, wird der Begriff Internetzwerk benutzt, wenn von einem Verbund beliebiger Teilnetze gesprochen wird. *Das* Internet wird durch folgende Eigenschaften charakterisiert (nach [FREISCHLAD, 2010, S. 3f]):

- Es ist ein Internetzwerk.

- Es basiert auf einem global eindeutigem Adressraum (Internet Protocol, kurz: IP).
- Durch den Protokollstapel besteht die Möglichkeit, Daten auszutauschen.
- Öffentliche und private Dienste höherer Schichten werden auf Basis der beschriebenen Infrastruktur bereitgestellt.

Als Schichtenmodell wird damit das vierschichtige TCP/IP-Modell mit Netzzugangs-, Vermittlungs-, Transport- und Anwendungsschicht verwendet (vgl. [TANENBAUM, 2003, S. 41ff]). Zusätzlich sollte beachtet werden, dass *das* Internet momentan das weltweit größte Internetzwerk mit den oben genannten Bedingungen ist.

TANENBAUM weist darauf hin, dass ein verteiltes System kein Netzwerk darstellt (vgl. [ebd., S. 2]). Innerhalb verteilter Systeme erscheinen mehrere Informatiksysteme durch spezielle Software, oft *middleware* genannt, für den Benutzer wie ein einziges System. Jedes einzelne Informatiksystem muss innerhalb eines verteilten Systems zwar mit den anderen Daten austauschen können, allerdings kann jedes einzelne System in unterschiedlichen Netzwerken verortet sein. Viele Angebote im Internet, etwa Suchmaschinen, Textverarbeitung usw., sind als verteilte Systeme realisiert. Für sich genommen ist das Internet jedoch kein verteiltes System. Netzwerke stellen prinzipiell nur die Infrastruktur für ein verteiltes System zur Verfügung.

2.4 Topologie

> »Die Topologie (wörtlich: Geometrie der Lage) eines Netzes (...) beschreibt in welcher Weise die Knoten durch Teilstrecken verbunden sind« [S. 39 STEIN, 2008, Schreibweise wie im Original].

Aus den unterschiedlichen physikalischen Trägermedien, die benutzt werden, um eine Verbindung herzustellen, sowie der Topologie selbst ergeben sich die folgenden Charakteristika.

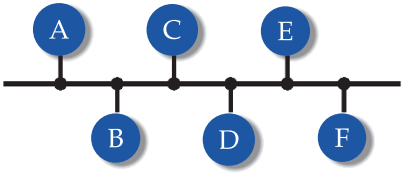
Bei einer Verbindung, die bspw. durch einen Kupferdraht, ohne Unterbrechung, direkt hergestellt wird (vgl. Abb. 2.1a, S. 10), werden die Daten auf der so entstandenen Teilstrecke von einem Sender zu nur einem möglichen Empfänger übertragen. Ein Netzwerk, das nur aus solchen direkten Teilstrecken aufgebaut ist, wird Teilstreckennetz (vgl. [ebd., S. 39]) oder Punkt-zu-Punkt-Netzwerk (vgl. [TANENBAUM, 2003, S. 15]) genannt. Wenn Daten über eine ungerichtete Funkverbindung übertragen werden, dann erhält nicht nur der vorgesehene Empfänger die Daten, sondern alle in Reichweite befindlichen Systeme empfangen die Nachricht. Ein Netzwerk, das aus solchen *geteilten* Verbindungen besteht, wird auch als Diffusionsnetz (vgl. [STEIN, 2008, S. 39]) bezeichnet.

Für den Nutzer ist es wichtig zu wissen, dass möglicherweise nicht nur Zwischensysteme die empfangenen bzw. gesendeten Daten weiterleiten und damit lesen können, sondern im Zweifel beliebig viele im Netzwerk befindliche Systeme. Neben Aspekten des Datenschutzes müssen auch technische Probleme beachtet werden. Bspw. kann in Diffusionsnetzen nur eine Nachricht gleichzeitig übertragen werden. Es muss demnach entschieden werden, welches System zu welcher Zeit senden darf. Außerdem müssen die Systeme entscheiden können, welche Nachrichten für sie selbst bestimmt sind.

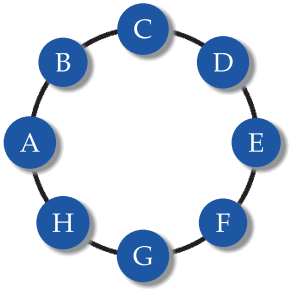
Aus technischer Sicht sind vor allem die Effizienz, Ausfalltoleranz und Skalierbarkeit eines Netzwerks von Interesse. Eine hohe Effizienz wird erreicht, wenn eine Nachricht im Durchschnitt möglichst wenige Zwischenknoten durchlaufen muss. Eine hohe Ausfalltoleranz ergibt sich, wenn der Ausfall eines Knotens die Funktionalität des Netzwerks nicht einschränkt (vgl. [ebd., S. 40f]). Besonders gut skalierbar sind Netze, deren Verkabelungsaufwand, also die Anzahl an Verbindungen, der entsteht, um neue Knoten aufzunehmen, möglichst gering ist. Der Begriff Verkabelung erscheint physikalisch nicht immer sinnvoll, da Verbindungen nicht zwangsläufig Kabel, sondern bspw. auch Funkverbindungen sein können.

In Abb. 2.1, S. 10 sind einige grundlegende Topologien aufgeführt. STEIN klassifiziert Topologien nach der Anzahl der Dimensionen in ein-, zwei- und mehrdimensionale. »Eine n-dimensionale Topologie lässt sich in einem n-dimensionalen Raum kreuzungsfrei aufzeichnen« [ebd., S. 39]. TANEN-

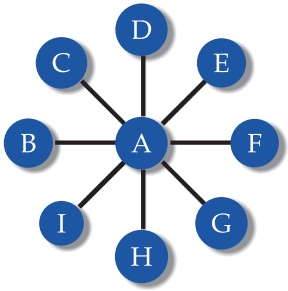
(a) *Punkt-zu-Punkt-Verbindung (P2P)*



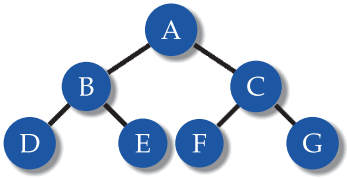
(b) *Bus*



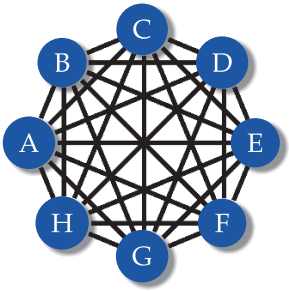
(c) *Ring*



(d) *Stern*



(e) *Baum*



(f) *Vollständig vermascht*

Abbildung 2.1: *Unterschiedliche Verbindungstopologien*

BAUM dagegen unterscheidet Topologien »nur« in Diffusions- und Teilstreckennetze (vgl. [TANENBAUM, 2003, S. 14ff]). Als grundlegenden Baustein kann prinzipiell die Punkt-zu-Punkt-Verbindung (*kurz:* P2P, vgl. Abb. 2.1a, S. 10) angesehen werden. Aus ihr werden komplexere Topologien, etwa vermaschte Netze[1], Ringe oder auch Bäume, zusammengesetzt. Da jede Verbindung *exklusiv* von nur zwei Systemen benutzt wird, kann eine hohe Effizienz erreicht werden. Allerdings führt der Ausfall eines Knotens oft zu Engpässen. Falls in Abb. 2.1e, S. 10 der Knoten A ausfällt, können zwischen dem Teilbaum B, D, E und C, F, G keine Daten mehr ausgetauscht werden.

In der Literatur ist nicht immer eindeutig, ob auch die Bustopologie (vgl. Abb. 2.1b, S. 10) aus P2P-Verbindungen besteht. Die tatsächliche Verkabelung einer Bustopologie kann tatsächlich den Eindruck erwecken, es würden einzelne, direkte Verbindungen zwischen den angeschlossenen Systemen bestehen (vgl. Abschnitt 2.4.2, S. 12). In einem Netzwerk, das nur aus P2P-Elementen aufgebaut ist, z. B. Abb. 2.1c, S. 10, kann eine Nachricht von Knoten A zu Knoten B übertragen werden, ohne das die anderen Knoten diese Nachricht ebenfalls erhalten. Theoretisch könnten die Knoten C und D sogar gleichzeitig eine andere Nachricht austauschen. Im Busnetz, wie in Abb. 2.1b, S. 10, sendet exklusiv A eine Nachricht zu B, die zugleich auch von allen anderen Knoten empfangen (und wieder verworfen) wird.

Demnach ist ein Bus konzeptionell betrachtet eher eine gemeinsame und lange Verbindung (Äther bzw. engl. *ether*), an die sich alle Systeme anschließen. Eine Nachricht ist immer auf der gesamten Verbindung empfangbar (vgl. [COMER und DROMS, 2002, S. 125]). Somit besteht ein Bus konzeptionell nicht aus P2P-Verbindungen. Da in heutigen technischen Realisierungen Bussysteme in Reinform nur noch selten anzutreffen sind, soll im weiteren Verlauf von gemeinsam genutzten Verbindungen gesprochen werden.

Außerdem werden Netzwerke in ihrer Skalierung (vgl. [TANENBAUM, 2003, S. 14f]) bzw. Größe unterschieden. Damit ist die tatsächliche physikalische Größe, also die Distanz, die zwischen den entfernten Knoten überbrückt wird, gemeint. Folgende Typen können angegeben werden (n.

[1] In einem vermaschten Netz hat mindestens ein Knoten mehr als zwei Verbindungen zu mehr als zwei anderen Knoten. In vollständig vermaschten Netzen (vgl. Abb. 2.1f, S. 10) besteht von jedem Knoten zu jedem anderen Knoten eine P2P-Verbindung.

[TANENBAUM, 2003, S. 16]) – wobei in der Literatur nicht explizit zwischen Netzwerk und Internetzwerk unterschieden wird:

PAN Personal area network, im Bereich weniger Meter, z. B. Bluetooth

LAN Local area network, im Bereich von einigen Metern (z. B. Heimnetzwerk in der Wohnung) bis zu wenigen Kilometern (z. B. Uni-Campus)

MAN Metropolitan area network, auf Städte oder Gemeinden beschränkt

WAN Wide area network, auf Länder oder Kontinente beschränkt

2.4.2 Logische Topologien

Letztlich ist in der Praxis nicht immer klar zu entscheiden, welche Topologie ein Netzwerk nutzt. Die sichtbare Verkabelung der Systeme kann bspw. eine andere Topologie nahelegen, als tatsächlich umgesetzt wird. Der weit verbreitete Ethernetstandard (sogenanntes DIX-Ethernet) zur Netzwerkverkabelung wurde bspw. ursprünglich in Bustopologie konzipiert (vgl. [COMER und DROMS, 2002, S. 126]). Die reale Verkabelung kann unter Umständen jedoch den Eindruck in Reihe hintereinander geschalteter Systeme, wie in [STEIN, 2008, S. 39, Bild 1.17] abgebildet, erwecken. Die »Kabel« stellen jedoch keine direkten Verbindungen her, sondern verlängern einen gemeinsam genutzten Äther. Der heute aktuelle Standard, *10BaseT* oder *TP-Ethernet*, benutzt physikalisch dagegen eine Sterntopologie mit einem zentralen System in der Mitte, obwohl logisch weiterhin Prinzipien einer gemeinsam genutzten Verbindung bestehen. Nach COMER und DROMS können in

> »einer bestimmten Netzwerktechnologie (...) verschiedene Anschlussarten [bzw. Topologien] verwendet werden. Die Technologie bestimmt die logische Topologie, während die physische Topologie von der Anschlussart vorgegeben wird. Die physische kann sich von der logischen Topologie unterscheiden« [COMER und DROMS, 2002, S. 170].

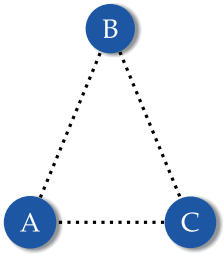
Hinzu kommen Netzwerke, die aus einer Art Mischform bestehen. Funknetze im LAN-Bereich (IEEE 802.11, vgl. [STEIN, 2008, Tab. 6.1, S. 188]) bspw.

können im sogenannten ad-hoc Modus oder mit einer Basisstation (access point) betrieben werden (vgl. [TANENBAUM, 2003, S. 68ff]). Sofern der ad-hoc Modus genutzt wird, kommunizieren die Systeme, wie bei einer P2P-Verbindung, (scheinbar) direkt untereinander (vgl. Abb. 2.2a, S. 14). Somit könnte ein vermaschtes Netz aufgebaut werden. Wird eine Basisstation verwendet, regelt diese zentral den Zugang und entsprechende Einstellungen, wie etwa die zu verwendende Frequenz (vgl. Abb. 2.2b, S. 14). Es entsteht der Eindruck einer Sterntopologie.

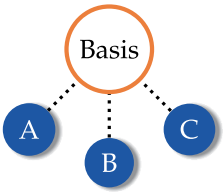
In Abb. 2.2, S. 14 stellen die gepunkteten Linien Funkverbindungen dar, die ungerichtet sind und sich radial ausbreiten. Physikalisch wird immer das selbe Trägermedium (elektromagnetische Wellen) genutzt. Ähnlich wie bei (analogen) Funkgeräten, können unterschiedliche Frequenzen genutzt werden, um gleichzeitig verschiedene Nachrichten, z. B. die Meldung eines Brandes an die Feuerwehr und eines Banküberfalls an die Polizei, übertragen zu können. Sofern jedoch die selbe Frequenz gewählt wird, entstehen Überschneidungen und es wird prinzipiell *dieselbe* Verbindung benutzt. Unabhängig vom Modus des Funknetzwerks entsteht so eine gemeinsam genutzte Verbindung (vgl. Abb. 2.2c, S. 14) – genau genommen stellt Abb. 2.2b, S. 14 einen Spezialfall des ad-hoc Modus dar, indem ein System die technischen Einstellungen entsprechend regelt.

Werden heutige lokale Netzwerke im Büro oder privatem Haushalt betrachtet, so wird schnell klar, dass es sich hier um komplexe Internetzwerke mit unterschiedlichsten Topologien handelt. Für alle in Abb. 2.3, S. 15 angeschlossenen Systeme entsteht der Eindruck, sie würden sich im selben Netzwerk befinden[2]. Die Systeme können Daten austauschen, z. B. um den Zugriff auf Dateien zu ermöglichen, Druckbefehle zu senden oder Daten aus dem Internet abzurufen. Zwar entsteht für den Endverbraucher oftmals der Eindruck, ein Drucker mit Netzwerkanschluss, ein Router, eine Funkbasisstation, ein Mobiltelefon, ein Fernseher usw. wären unterschiedliche Geräte mit speziellen Funktionen, allerdings können sie aus informatischer Sicht (meist) als vollwertige Informatiksysteme betrachtet werden. Die tatsächliche Funktion für den Endnutzer ist hier unerheblich. Abb. 2.3, S. 15 zeigt außerdem, dass eine Topologie nicht zwangsläufig die tatsächliche

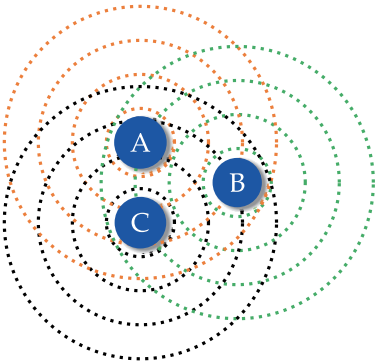
[2] Alle Systeme müssen innerhalb eines lokalen Internetzwerks mit dem gleichen Referenzmodell bzw. Protokollstapel, etwa TCP/IP, arbeiten, um problemlos miteinander kommunizieren zu können.



(a) *Ad-hoc-Verbindungen*



(b) *Funknetzwerk mit einer Basisstation*

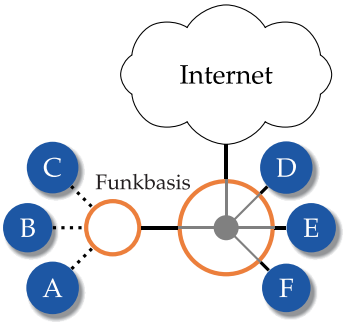


(c) *Funknetzwerke als Bustopologie*

Sofern alle Nutzer die gleichen Einstellungen benutzen, entsteht (auch im ad-hoc Modus) ein Funknetzwerk, das prinzipiell wie eine Bustopologie organisiert ist, da die sich radial ausbreitenden Funkwellen, hier durch gepunktete Kreise symbolisiert, einer gemeinsamen Verbindung für alle Knoten entsprechen.

Abbildung 2.2: *Darstellung möglicher Verbindungen in Funknetzwerken (angelehnt an [*TANENBAUM*, 2003, Abb. 1-35, S. 69], IEEE 802.11)*

geometrische Verortung im physikalischen Raum meint, sondern die Verbindungen konzeptionell aufgreift, ähnlich eines Streckennetzplans, der Stationen mehrerer Straßenbahnlinien abbildet. Das per Funkverbindung angeschlossene System A könnte sich bspw. direkt neben dem per Kabelverbindung angeschlossenem System E befinden.



In der nebenstehenden Abbildung werden zur Verdeutlichung Endsysteme unabhängig von ihrer Funktion für den Benutzer als gefüllte Kreise verdeutlicht. Systeme, die das Netzwerk erweitern, etwa Funkbasisstationen, sind als weiße Kreise gezeichnet, die den Blick auf die innenliegende Topologie ermöglichen.
Der Zugang zu *dem* Internet wird durch ein System in der Mitte hergestellt, das dadurch oft auch als Router bezeichnet wird. Das Internet wird als eine Wolke dargestellt. Es sollte klar sein, dass diese *Wolke* symbolisch für Verbindungen zu weiteren Zwischenknoten und möglichen Endknoten steht.

Abbildung 2.3: *Darstellung eines typischen lokalen Internetzwerks in einem privaten Haushalt, bestehend aus (gepunkteten) Funk- und Kabelverbindungen*

Neben der tatsächlichen, *technischen* Installation eines Netzwerks entstehen, durch die Benutzung von konkreten Angeboten bzw. Diensten, Verbindungen mit unterschiedlichen Topologien. Benutzt Lisa[3] einen Instant Messenger (*kurz:* IM) um Emilie ins Kino einzuladen, so entsteht für die beiden der Eindruck, sie würden eine direkte P2P-Verbindung benutzen. Dabei wohnen sie weit voneinander entfernt und befinden sich in den unterschiedlichsten Netzwerken (vgl. Abb. 2.4, S. 17, Lisa sei Knoten L, Emilie Knoten E). Selbst wenn sie durch Verschlüsselungs- und Authentifizierungslösungen dafür sorgen, dass tatsächlich nur sie beide ihre Nachrichten

[3]Die verwendeten Namen sind frei erfunden, könnten ebenso männlich sein und dienen damit nur der Illustration.

lesen können, werden die Daten der Nachrichten durch verschiedene Internetzwerke und *das* Internet geleitet. Die rot markierte Linie stellt den Weg der Verbindung dar. Es wird keine direkte P2P-Verbindung benutzt (vgl. Abb. 2.4, S. 17).

Es scheint unterschiedliche Abstraktionsebenen von Topologien zu geben. Auf der Ebene konkreter Anwendungen kann eine Topologie wahrgenommen werden, die durch die physikalische bzw. technische Ebene nicht umgesetzt wird. Daraus können sich unterschiedliche Probleme ergeben – bspw. könnten die Daten der Kommunikation zwischen Lisa und Emilie von Maria (Knoten M) unbemerkt mitgelesen und missbraucht werden. Tatsächlich können sämtliche Zwischenknoten, die durchlaufen werden, Daten mitlesen. Je nach Betrachtung wird eine andere *logische* Topologie (vgl. [*Topologie (Rechnernetze)* 2014]), die je nach Abstraktion oder konkretem Nutzen unterschiedliche Ausprägungen beinhaltet, umgesetzt. Die logische Topologie muss dabei nicht mit einer tatsächlich vorhandenen physikalischen Verbindung übereinstimmen, sondern kann durch Software umgesetzt werden.

Hieraus ergeben sich für den Benutzer zum Teil gravierende Problematiken. Sofern Lisa und Emilie ihre Kommunikation ausreichend sichern, können Angreifer nichts mit den abgehörten Daten anfangen. Wenn die beiden jedoch nur die Abstraktionsschicht, die die Software des Instant Messengers liefert, betrachten, könnten sie glauben, dass sie direkt miteinander kommunizieren würden und eine Verschlüsselung womöglich unwichtig sei. Um potentielle Risiken durch die Kommunikation im Internet zu verstehen, müssen sowohl die Eigenschaften der unterschiedlichen Topologien verstanden, als auch die unterschiedlichen Abstraktionsschichten der übertragenen Daten noch genauer betrachtet werden.

2.5 Protokolle und Pakete

2.5.1 Hierarchische Organisation von Protokollen

Bisher wurde vor allem auf die physikalischen Grundlagen von Verbindungen und sich daraus ergebenden Netzwerkstrukturen eingegangen. Allerdings müssen darüber hinaus auch die ausgetauschten Daten betrach-

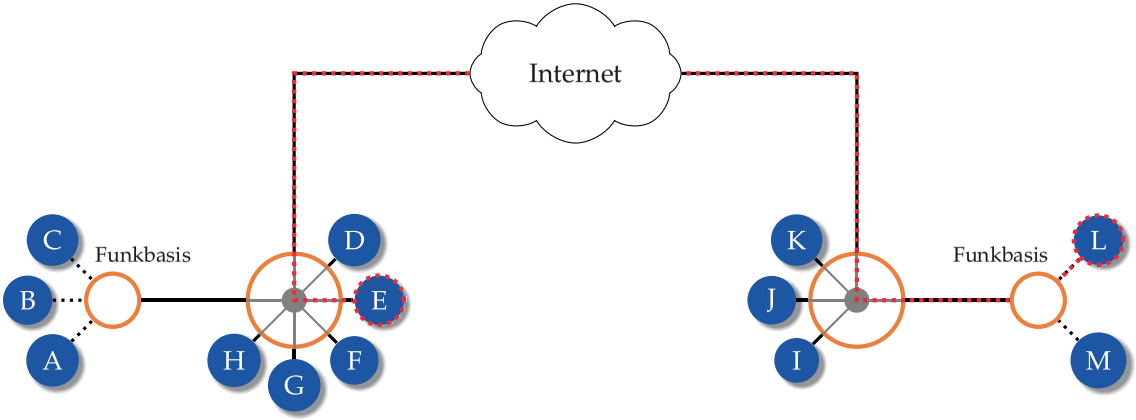


Abbildung 2.4: *Endknoten aus zwei unterschiedlichen Internetzwerken können durch das Internet miteinander kommunizieren*

tet werden. Das Abrufen von Webseiten, Musik, Videos, Textdateien oder die Steuerung von Modelleisenbahnen oder Atomkraftwerken sind nur wenige Beispiele für Anwendungsszenarien, in denen es notwendig ist, Daten zwischen Informatiksystemen auszutauschen. Es wird deutlich, dass sich durch die vielfältigen Einsatzmöglichkeiten auch Anforderungen an den Datenaustausch ergeben – bspw. könnte es dem Mitarbeiter eines Atomkraftwerks wichtig sein, dass die Meldung eines schweren Unfalls im Kernreaktor eine höhere Priorität zuteil wird als dem Abruf des abendlichen Fernsehprogramms. Dass sich, durch die unterschiedlichen Topologien bzw. physikalischen Bedingungen, unterschiedliche Anforderungen hinsichtlich der Kommunikation ergeben könnten, haben die vorherigen Abschnitte bereits deutlich gemacht.

Die zuvor beschriebenen Überlegungen legen zwei mögliche Betrachtungsebenen nahe: die der Anwendung(-ssituation) und die der Hardware. Etwa im Falle von Emilie und Lisa (vgl. Abb. 2.4, S. 17) muss auf beiden Ebenen jeweils eine vollkommen andere logische Topologie umgesetzt werden. Dennoch sind beide Ebenen voneinander abhängig. Die Daten müssen über die gegebene Infrastruktur übertragen werden, sollen aber zugleich eine Art direkter Kommunikation zwischen Emilie und Lisa ermöglichen. Bedingung dafür ist, dass die beiden sich verständigen können – typischerweise indem sie aus Buchstaben unter Beachtung der Regeln einer Sprache Wörter und Sätze bauen, im Rahmen der Netzwerktechnik auch Protokoll genannt. »Basically, a protocoll is an agreement between the communicating parties on how communication is to proceed« [TANENBAUM, 2003, S. 27].

Daneben müssen aber auch die verwendeten Systeme sich auf ein Protokoll einigen und nicht zuletzt die Anforderungen der jeweiligen Netzwerkinstallation beachten. Emilie und Lisa wollen sich aber keine Gedanken machen, wie ihre Daten übertragen werden, sondern sich nur untereinander einigen. Daher sollte es eine Möglichkeit geben, die Aspekte der Kommunikation zwischen Emilie und Lisa von anderen, für die Übertragung notwendigen, Aspekten trennt. Daraus könnten jeweils einzelne, aufeinander aufbauende und abhängige Protokolle entstehen, die untereinander mit Schnittstellen kommunizieren können (vgl. [ebd., Abb. 1-14, S. 29]).

Damit wurde auf einfache Weise ein *Schichtenmodell* definiert (vgl. [ebd., S. 26ff; STEIN, 2008, S. 22ff] und Abb. 2.5, S. 19), das aus zwei, allgemein n beliebigen, Schichten besteht. Jede Schicht n scheint mit der entsprechenden

Emilie und Lisa wollen miteinander reden. Sie benutzen einen IM, der, um eine direkte Verbindung zu ermöglichen, ein entsprechendes Protokoll in der Software-Schicht umsetzt. Die Entwickler des IM mussten sich nicht um die Bedingungen der Netzwerkinstallation kümmern. Innerhalb der jeweiligen Schicht entsteht der Eindruck, sie würden Daten direkt mit der entsprechenden Schicht des Kommunikationspartners austauschen. Tatsächlich werden die Daten über eine Schnittstelle zur Hardware-Schicht geleitet, welche in einem eigenen Protokoll die technischen Voraussetzungen des Netzwerks beachtet und die Daten über die vorhandenen Verbindungen überträgt.

In heute existierenden Umsetzungen für Netzwerke, etwa TCP/IP, wird die Eingabe von Emilie und Lisa nicht als eine mögliche Schicht berücksichtigt. Letztlich stellt aber schon die Eingabe der Nachricht einen Schritt der Kommunikation dar, deren Auswirkungen in den technischen Realisierungen nicht näher untersucht werden – daher hier nur als gedachte *Schicht* abgebildet.

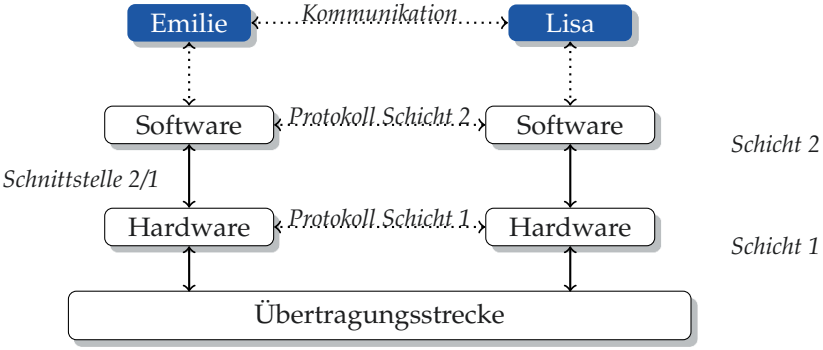


Abbildung 2.5: *Einfaches Schichtenmodell mit zwei Schichten – die erste Schicht regelt die Belange der Hardware, in der zweiten Schicht kann Software realisiert werden (vgl. [*TANENBAUM*, 2003, Abb. 1-13,1-14; S. 27ff])*

Schicht n des Kommunikationspartners direkt zu kommunizieren. Dabei werden die Daten der Kommunikation von jeder Schicht – auch Instanz genannt – an die darunter liegende weitergereicht bzw. von der darunter lie-

genden entgegengenommen. »The fundamental idea is that a particular piece of software (...) provides a service to its users but keeps the details of its internal state and algorithms hidden from them« [TANENBAUM, 2003, S. 26]. Jede Schicht ist für sich genommen unabhängig von den anderen Schichten, so dass eine Standardisierung bzw. Einigung auf zentrale Protokolle nur für die jeweils betrachtete Schicht und nicht das komplexe Gesamtsystem getroffen werden müssen (vgl. [STEIN, 2008, S. 22]). Ein Schichtenmodell folgt damit dem Prinzip von *teile und herrsche*, um ein komplexes System strukturiert in einfache, *beherrschbare* Teile zu zerlegen.

»A set of layers and protocols is called a network architecture« [TANENBAUM, 2003, S. 28]. In einer gegebenen Netzwerkarchitektur muss klar definiert sein, wie Geräte auf der physikalischen Ebene arbeiten müssen und wie Protokolle für die einzelnen Schichten implementiert werden können. »Die Gesamtheit der Protokolle aller Schichten wird als Protokollstapel (...) bezeichnet« [STEIN, 2008, S. 25].

2.5.2 Pakete und Rahmen

Die beiden bedeutendsten Schichtenmodelle in der Netzwerktechnik, das OSI- (Open Systems Interconnection) und das in dieser Arbeit verwendete TCP/IP-Referenzmodell (vgl. [TANENBAUM, 2003, S. 37ff]), benutzen sieben bzw. vier anstelle von nur zwei Schichten. Heutige Anforderungen an Netzwerkarchitekturen sind so komplex, dass eine Aufteilung lediglich in Hard- und Software nicht ausreicht. In jeder Schicht wird mindestens ein spezielles Protokoll realisiert. Dadurch entstehen zusätzliche Daten, die für eine Kommunikation innerhalb der Schicht notwendig sind. Solche Metadaten, z. B. die Empfängeradresse, werden im sogenannten *Header* gespeichert (vgl. [ebd., S. 29]). Sie gehören also nicht zur eigentlichen Nachricht, sondern stellen die Übertragung sicher. Jede Schicht hat ihren eigenen Header, der als zusätzliches Datenfeld vor der eigentlichen Nachricht übertragen wird. Dadurch entsteht ein Datagramm bestehend aus den Headern der jeweiligen Schicht und der tatsächlichen Nachricht (vgl. Abb. 2.6, S. 21).

Nun gilt es zu beachten, dass ein solches Datagramm bei der Übertragung zu einem Endknoten unter Umständen viele verschiedene Knoten durch-

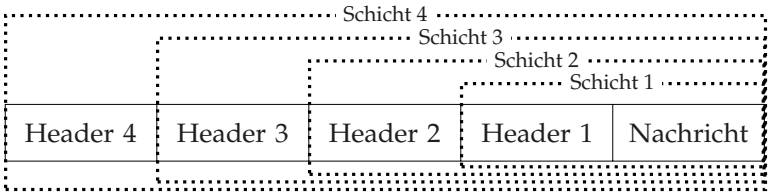


Abbildung 2.6: *Datagramm bei Verwendung eines vierschichtigen Modells*

laufen muss (vgl. Abb. 2.4, S. 17). Daraus ergeben sich unterschiedliche Aspekte.

Paketvermittlungsnetz

In vielen Netzwerken werden »nicht ständig beliebige Datenmengen« [COMER und DROMS, 2002, S. 101] übertragen, sondern »vielmehr teilt das Netzsystem die Daten in kleine Blöcke – so genannte Pakete (...) – auf, die einzeln gesendet werden« [ebd., S. 101]. Im Gegensatz dazu gibt es auch die Möglichkeit, eine exklusive Nutzung zu gestatten, etwa wie beim alten analogen Telefonanschluss üblich[4]. Allerdings zeigt sich, dass sofern mehrere Nutzer dieselbe Ressource bzw. dasselbe Netzwerk nutzen möchten, andere Systeme durch die exklusive Nutzung unnötig lange blockiert werden. Wie schon zu Abb. 2.1b, S. 10 beschrieben, müssen die Systeme nicht nur regeln, wer empfangen darf, sondern auch wer senden darf. Durch die Aufteilung in einzelne Pakete ist es möglich, allen einen *gerechten* Zugang zur gemeinsamen Ressource, z. B. dem Äther, zu gewähren (vgl. [ebd., S 101f]). Es werden gewissermaßen abwechselnd kleine Datenmengen übertragen. Dadurch verlängert sich zwar für den einzelnen die Übertragungsdauer, jedoch können alle *quasi*-gleichzeitig übertragen.

Daneben gibt es weitere Überlegungen, die ein Paketvermittlungsnetz favorisieren. Innerhalb dieser Arbeit kann darauf im Detail nicht näher

[4] In analogen Telefonnetzen kann von einem Anschluss nur ein Gespräch geführt werden. Ein zweites Telefon kann entweder dem selben Gespräch lauschen oder muss warten bis die Leitung wieder frei ist.

eingegangen werden (vgl. hierzu die Fachliteratur). *Das* Internet arbeitet ebenfalls mit Paketen.

Hardware-Rahmen

Bei der Übertragung durch komplexe Internetzwerke müssen viele unterschiedliche Knoten das Datagramm weiterleiten. Jedes Netzwerk hat unterschiedliche technische Voraussetzungen, so dass z. B. an die Größe des Pakets explizite Vorgaben bestehen. Der Begriff Paket oder Datagramm soll das allgemeine Konzept der Bündelung von Daten (und Metadaten) in einer einzelnen (kleinen) Datenstruktur umfassen. Sofern dagegen durch die Hardware spezifische Anforderungen an ein Paket definiert werden, soll von Rahmen gesprochen werden (vgl. [COMER und DROMS, 2002, S. 104]). So kann es notwendig werden, dass die Schichten unterschiedliche Problemstellungen in ihren Protokollen beachten müssen. Da die maximale Größe eines Rahmens feststeht, muss das Datagramm im Zweifel auf mehrere Rahmen aufgeteilt werden. Durch verschiedene Verfahren können Fehler in der Übertragung erkannt oder je nach Bedarf die richtige Reihenfolge der Rahmen sichergestellt werden (vgl. [ebd., S. 107ff]).

Routing

Rahmen müssen in großen Internetzwerken lange Wege zurücklegen, um zu ihrem Ziel zu kommen. In einer Bustopologie entscheiden die angeschlossenen Systeme, ob der Rahmen für sie bestimmt ist. In P2P-Netzen muss der jeweilige Knoten entscheiden, wie er den Rahmen weiterleitet. Dafür ist es notwendig, den Rahmen mindestens bis zur Vermittlungsschicht zu betrachten. Der Header eines IP-Pakets beinhaltet unter anderem die Zieladresse. Jeder vermittelnde Knoten muss Algorithmen ausführen, um zu bestimmen, wie das Paket weiterzuleiten ist.

Das Finden eines Weges vom Sender zum Empfänger wird in Netzwerken *Routing* genannt. Im IP-Protokoll werden die Adressen entsprechend der Zugehörigkeiten zu Internetzwerken vergeben. Somit kann ein vermittelnder Knoten bzw. *Router* durch den Vergleich der Zieladresse mit seiner eigenen grob entscheiden, in welches Teilnetzwerk er das Paket weiterlei-

ten muss. Detailliertere Ausführungen bezüglich Routing sind im Rahmen dieser Arbeit nicht notwendig (vgl. [STEIN, 2008, Kap. 9.4]).

TCP/IP Referenzmodell

In *dem* Internet wird das TCP/IP Referenzmodell benutzt. Es hat die Netzzugangs-, Vermittlungs-, Transport- und Anwendungsschicht.

- Die Netzzugangsschicht regelt den Umgang mit der konkreten Netzwerkhardware, z. B. die Unterschiede zwischen kabelgebundenen P2P-Netzwerken und kabellosen Bus-Netzwerken, und gibt so Rahmen vor.
- Auf der Vermittlungsschicht wird in erster Linie das Internet-Protokoll (IP) eingesetzt. Jeder Knoten erhält eine eindeutige Zahl als Adresse. Die Pakete der höheren Schichten werden an die Rahmen angepasst, also z. B. aufgeteilt, und in Richtung des Zielsystems gesendet bzw. entsprechend empfangen (vgl. [ebd., S 353f]).
- Die Transportebene setzt Protokolle um, die die Art der Verbindung anpassen sollen. Dafür werden heute fast ausschließlich TCP (Transmission Control Protocol, verbindungsorientiert) und UDP (User Datagram Protocol, verbindungslos) eingesetzt (vgl. [TANENBAUM, 2003, S. 43]).
- In der Anwendungsschicht liegen die Protokolle der jeweiligen Anwendungssoftware, die genutzt werden soll. Typischerweise wird jedem Protokoll eine Nummer (*port*) zur Identifikation zugewiesen.

In der Praxis benötigt der Anwender die Adresse des Zielsystems und die Portnummer des Protokolls, das er erreichen möchte[5]. Die Hardwareprotokolle werden durch das Betriebssystem umgesetzt. Im Rahmen dieser Arbeit kann nicht auf sämtliche Protokolle des TCP/IP Referenzmodells im Detail eingegangen werden. Daher sei zur Vertiefung auf die zu Beginn dieses Abschnitts erwähnte Fachliteratur verwiesen.

[5] Oftmals wird durch vorkonfigurierte Anwendersoftware die Portnummer automatisch gewählt, so dass nur noch die Adresse des Zielsystems eingegeben werden muss.

Dienste haben für den Endanwender eine große Bedeutung. So unterscheidet sich im Detail bspw. das *post office protocol* (*kurz:* POP) vom *internet message access protocol* (*kurz:* IMAP) – dennoch sind beide für das Abholen von E-Mails auf einem entfernten System geeignet. Allgemein umfasst ein Dienst eine abstrahierte Funktion für den Nutzer. Demnach hat ein Dienst eine klare Funktionskomponente, etwa den Empfang einer Webseite per *hypertext transport protocol* (*kurz:* HTTP). Somit wird durch den Dienst der konkrete Nutzen für den Anwender definiert. Generell werden unter Diensten nicht nur die bereitgestellten Funktionen eines Protokolls in der Anwendungsschicht verstanden, sondern jede Schicht stellt durch das verwendete Protokoll Funktionen an höhere Schichten zur Verfügung (vgl. [STEIN, 2008, S. 25ff]).

Außerdem wird zwischen verbindungsorientierten und verbindungslosen Diensten unterschieden. Verbindungsorientierte Dienste können etwa mit einer Telefonverbindung verglichen werden. Es wird eine Verbindung zwischen zwei Endknoten hergestellt, indem einmal eine Nummer gewählt wird und der Kommunikationspartner den Hörer abnimmt. Die Verbindung bleibt bestehen, bis ein Gesprächspartner die Verbindung beendet. Ein verbindungsloser Dienst sendet Daten aufgeteilt in vielen Paketen als wären es Postkarten – jede Postkarte enthält die Empfängeradresse, jedoch können einzelne Karten verspätet ankommen oder verloren gehen (vgl. [TANENBAUM, 2003, S. 32ff]). Dennoch nutzen beide Möglichkeiten die selben Rahmen, um ihre Daten zu senden. Die jeweiligen Protokolle müssen dafür Sorge tragen, dass dennoch die entsprechenden Auflagen an die Verbindung beachtet werden.

Zusätzlich erscheint der Begriff des *Angebots* gerade im Kontext von Cyber-Mobbing sinnvoll, da immer mehr Dienste keine klar einzugrenzende Funktionskomponente besitzen. Bspw. erscheint Empfang und Versand von E-Mails durch den HTTP-Dienst abgelöst, sofern entsprechende, *webbasierte* Software der großen Anbieter benutzt wird. Aber auch komplexe Angebote, wie Foren oder soziale Netzwerkdienste (vgl. Abschnitt 3.2.1, S. 42), scheinen viele mögliche Dienste und Funktionen innerhalb einer Software zu bündeln, um etwas für die Nutzer Neues und Interessantes zu schaffen. Gerade durch die (Weiter-)Entwicklung von Browsern und entsprechenden Programmierumgebungen werden immer mehr Funktionskomponenten

oder bestehende Dienste gebündelt. Es entstehen teilweise eigene Schnittstellen, die die Kommunikation mit bestimmten Funktionen einer Webseite durch den HTTP-Dienst ermöglichen. Prinzipiell könnten solche Erweiterungen als neue Schichten aufgefasst werden – dies findet jedoch bisher keine Berücksichtigung. Solche, typischerweise über den Browser angebotene, Software soll als Angebot im Internet bezeichnet werden.

2.6 Sicherheitsaspekte aus informatischer Sicht

An Netzwerkarchitekturen werden viele verschiedene Bedingungen gestellt. Sie müssen möglichst schnell sein oder eine günstige Verkabelung ermöglichen. Einige eher technische Bedingungen wurden in den vorherigen Abschnitten aufgezeigt. Da die Übertragung von Daten in *dem* Internet durch ein Schichtenmodell realisiert wird, kann der Endanwender Dienste und Angebote nutzen, ohne ein gesamtes Verständnis für die Übertragung besitzen zu müssen. Daher weiß er möglicherweise nicht, dass Pakete auf dem Weg von einem Endknoten zu einem anderen Endknoten von vielen Zwischenknoten betrachtet und weitergeleitet werden müssen. Für ihn erscheint eine direkte Verbindung realisiert. Prinzipiell werden Mechanismen benötigt, die die logische Topologie eines Anwendungsprotokolls gegen ungewollte Effekte durch die tatsächliche Topologie der darunter liegenden Schichten absichern. Emilie und Lisa möchten schließlich zu Recht nicht sämtliche Protokolle aller Schichten selbst entwickeln, um die Übertragung der Daten nach ihren Wünschen zu gestalten. Immer wieder gibt es Schlagzeilen über *Verbrechen* im Internet – es werden Kreditkartendaten missbraucht, E-Mails mitgelesen oder die Telefone von Regierungsmitgliedern abgehört (vgl. [HOLLAND, 2014]). Aus Nutzersicht gibt es ein Interesse daran, ein *sicheres* Internet benutzen zu können.

Neben den Interessen des Einzelnen gibt es eine weitere – zumeist wesentlich einflussreichere – Gruppe, die Netzwerke sicher gestalten möchte: Wirtschaftsunternehmen. Um vor Wirtschaftsspionage und ähnlichen Übergriffen, aber z. B. auch Übertragungsfehlern in sensiblen Bereichen – etwa bei Banküberweisungen – zu schützen, werden bzw. wurden Mechanismen und Konzepte entwickelt, um eine *sichere* Übertragung zu gewährleisten. Allerdings ist der Begriff *Sicherheit* nicht absolut zu definieren. Individuell

gibt es unterschiedliche Anforderungen und Aspekte an den Status *sicher* (vgl. [COMER und DROMS, 2002, Kap. 37.2]). Z. B. könnten an ein Netzwerk, bestehend aus einem Drucker und einem Computer ohne weitere Verbindungen, weniger hohe Sicherheitsbemühungen als an einen von hunderten verschiedenen Nutzern erreichbaren Drucker angestrebt werden. Im letzteren Fall möchte der Besitzer möglicherweise Kosten regulieren und den Zugriff beschränken, wobei im ersten Fall der Besitzer selbst die direkte Kontrolle hat.

Deutlich hervorzuheben ist, dass Sicherheit immer relativ zu bewerten ist. Es bedeutet weder, dass Angriffe unmöglich sind, noch dass es für immer sicher ist. Gerade aus didaktischen Gründen werden daher im Folgenden allgemeine Konzepte oder *fundamentale Ideen* (vgl. Abschnitt 2.7, S. 31), die dennoch als zeitlich invariante Basis der Netzwerksicherheit identifiziert werden können, herausgestellt.

2.6.1 Sicherheitsstandards in (offenen) Internetzwerken

Typischerweise werden Sicherheitsstandards immer dann als unerlässlich beschrieben, wenn Angriffszenarien möglich werden. Sowohl STEIN als auch COMER und DROMS unterscheiden dafür zwischen offenen und geschlossenen Internetzwerken. Gemeint ist damit, dass in offenen Internetzwerken den Endknoten die möglichen Zwischenknoten unbekannt sind bzw. sie deren Glaubwürdigkeit nicht prüfen können. Dies kann sowohl in Funknetzen aber auch in Kabelnetzen (etwa in Netzwerken, die die Stromleitung als Übertragungsmedium nutzen oder wenn der Internetzugang durch das (ursprünglich) in Bustopologie organisierte TV-Kabelnetz hergestellt wird (vgl. [TANENBAUM, 2003, S. 175f])) und nicht zuletzt in *dem* Internet der Fall sein. Fragwürdig ist, ob die Unterscheidung zwischen offenen und geschlossenen Internetzwerken tatsächlich sinnvoll ist, um Sicherheitsstandards zu unterscheiden. TANENBAUM gibt zu bedenken, dass die meisten Sicherheitsprobleme durch falsch informierte oder böswillig handelnde Mitarbeiter bzw. Mitglieder eines eigentlich geschlossenen Internetzwerks entstehen (vgl. [ebd., S. 723ff]). Dennoch muss definiert werden, was in welchem Kontext zu *schützen* ist.

Zunächst werden rein technische Aspekte der Sicherheit betrachtet, indem die möglichen Bedrohungen herausgestellt und daraus allgemeine Sicherheitsziele abgeleitet werden. Die aufgelisteten fünf Ziele werden in der Literatur oft als grundlegende von Internetzwerken zu erreichende Ziele beschrieben (vgl. [STEIN, 2008, S. 175ff; FREISCHLAD, 2010, S. 36ff; COMER und DROMS, 2002, Kap. 37]) – allerdings werden die Ziele selten eindeutig standardisiert. Daher liegen dieser Arbeit in erster Linie die im Folgenden beschriebenen Anforderungen an Informationssicherheit der *International Telecommunication Union* (*kurz:* ITU) nach [FREISCHLAD, 2010, S. 36] zu Grunde.

Authentifikation An einer Kommunikation beteiligte Endknoten müssen sich *ausweisen* können, da ansonsten beliebige Endknoten vorgeben könnten, den gewünschten Dienst, möglicherweise gefälscht, vorzuhalten.

Geheimhaltung An der Kommunikation notwendigerweise oder böswillig beteiligte Zwischenknoten können die Nachricht des Pakets ebenfalls lesen. Die Nutzung der eigentlichen Nachricht durch andere Knoten muss unterbunden werden.

Integrität Sowohl böswillige Veränderungen durch andere Knoten als auch Übertragungsfehler können Daten verfälschen. Die Echtheit der Daten muss bestätigt werden können.

Die ersten drei Ziele sind unabhängig vom Dienst und Nutzer wichtige Ziele, die in jedem Internetzwerk eingehalten werden sollten. Sie stellen nicht nur einen Schutz gegen böswillige Attacken, sondern auch gegen fehlerhafte Software, dar.

Nichtabstreitbarkeit Es ist unklar, ob Pakete tatsächlich gesendet oder angekommen sind. Durch Angriffe oder Übertragungsfehler könnten sie verloren gegangen sein. Es muss eine Bestätigung über den Versand und Empfang geben.

Zugriffskontrolle Auch in offenen Netzwerken sind Inhalte für den freien, eingeschränkten oder ausschließlichen Zugriff vorgesehen. Möglicherweise sind die Einträge eines Tagebuchs dem Verfasser exklusiv

vorbehalten, wohingegen die Urlaubsfotos der gesamten Familie zur Verfügung stehen sollen. Der Zugriff auf Dienste muss geregelt und verfügbar sein.

Die Nichtabstreitbarkeit ist nicht für alle Dienste notwendig bzw. sinnvoll. Bei einer Videoübertragung können bspw. einzelne Pakete verloren gehen, ohne dass die Wiedergabe des Videos gestört wäre. Für den Nutzer ist es zunächst nicht von Interesse zu erfahren, ob die Daten tatsächlich abgesendet wurden. Er möchte nur das Video sehen. Dagegen ist bei einer Geldüberweisung wichtig, ob die Überweisung getätigt und empfangen wurde. Gerade bei großen Summen könnte es sonst zu Missverständnissen kommen.

Auch eine Zugriffskontrolle ist nicht immer notwendig. Bestimmte Dienste sollen sogar für jeden abrufbar sein. Allerdings sollte dem Nutzer und vor allem dem Anbieter bewusst sein, dass eine Kontrolle möglich ist, sofern sie von Nöten wäre.

2.6.2 Psychologische Aspekte der Sicherheit in Internetzwerken

Der bisher dargestellte Blick auf Sicherheit in Internetzwerken orientiert sich stark an den technischen Voraussetzungen. Somit könnte der Eindruck entstehen, Sicherheit wäre durch das Ausmerzen sämtlicher *Lücken* in der Modellierung bzw. Implementierung von Netzwerken zu erreichen. Die Realität ist allerdings wesentlich komplexer und soll nur kurz skizziert werden.

Eine gute Sicherheitsarchitektur benötigt die folgenden vier Elemente (vgl. [ANDERSON, 2008, S. 4f]):

- Einen Verhaltenskodex, so dass Handlungsabläufe und Zuständigkeiten klar sind,
- notwendige Geräte, wie etwa Fingerabdrucksensoren oder Metalldetektoren an Flughäfen,
- Vertrauen, sowohl empirisch als auch gefühlt,
- Motivation.

Die beschriebenen vier Elemente greifen ineinander und müssen gegeneinander abgewogen werden. Dies kann bspw. dazu führen, dass Menschen mehr Angst haben, dass in ihr Haus eingebrochen oder ihr Auto gestohlen wird, als davor, dass jemand ihre privaten E-Mails mitlesen könnte. Somit entsteht zwar eine Motivation, Geräte und Kodexe zu entwickeln, um Einbrecher daran zu hindern den materiellen Besitz zu entwenden, aber über unverschlüsselte E-Mail-Kommunikation können Bewegungsprofile, Beziehungsstatus etc. erfahren werden, um einbrechen zu können, wenn niemand zu Hause ist – denn Einbrecher haben vor nichts mehr Angst, als davor, auf frischer Tat erwischt zu werden (vgl. [ebd., S. 10f]).

Wenn von Sicherheit in Internetzwerken gesprochen wird, dann muss demnach auch über psychologische Aspekte diskutiert werden – denn rein praktisch ist es möglich die zuvor genannten Ziele zu erreichen (vgl. Abschnitt 2.6.3, S. 31). Doch zum einen müssen die Nutzer davon überzeugt werden, solche Techniken auch zu benutzen und in ihren alltäglichen *Kodex*, so wie das Abschließen des Hauses, aufzunehmen. Zum anderen ist das alltäglichere Problem vor allem das sogenannte »Phishing«. Menschen werden angerufen, erhalten gefälschte E-Mails oder werden auf eine modifizierte Webseite geleitet, um Passwörter zu nennen, Verträge abzuschließen usw. (vgl. [ebd., Kap. 2]). ANDERSON benennt Nutzbarkeit als das Hauptaugenmerk heutiger Sicherheitsüberlegungen. Daher werden Passwörter in der heutigen Alltagswelt zur Identifizierung und Absicherung eingesetzt, obwohl bekannt ist, dass Passwörter häufig vergessen und daher zu einfache verwendet werden. Somit sind sie im Gegensatz zu anderen Verfahren viel *unsicherer* (vgl. [ebd., Kap. 2.4]).

Es wird deutlich, dass Sicherheit in hohem Maße vom Nutzer selbst abhängt und nicht nur vom im Zweifel böswilligen Anbieter. Außerdem benötigt der Benutzer Vertrauen in die Sicherheit seines Handelns.

> »Vertrauen aber kann enttäuscht und getäuscht werden. Mit der Komplexität (…) steigt die Unsicherheit der Teilnehmer. Vertrauensbildende Maßnahmen sind erforderlich. Technische Sicherheit soll Vertrauen dort stärken, wo es enttäuscht werden kann. Fehlendes Vertrauen in einen Prozess wird damit durch Vertrauen in ein technisches Verfahren kompensiert« [KOUBEK, 2006, S. 25].

Eigentlich wird so vom handelnden Individuum die Kompetenz abverlangt, das Vertrauen in technische und soziale bzw. psychologische Aspekte von Sicherheitsarchitekturen einschätzen und abwägen und daraus einen entsprechenden Verhaltenskodex ableiten zu können. Es ist zu klären, ob das Vertrauen in ein *technisches Verfahren* zu höherer Sicherheit führen kann, selbst wenn das faktische Verständnis über die verwendeten Verfahren und damit die eigentliche Einschätzung in sicher oder unsicher nicht gegeben ist. Letztlich ist Sicherheit eben ein Gefühl, das individuell befriedigt wird. Unwissenheit kann somit zu einem Vertrauen führen, das unter objektiven Gesichtspunkten unsinnig erscheint. Sicherheitsprobleme können mit Hilfe informatischer Werkzeuge gelöst werden. Dennoch entscheiden psychologische Aspekte, wie etwa die Motivation oder das Vertrauen der handelnden Individuen, darüber, wie umfassend Sicherheitsverfahren umgesetzt bzw. eingesetzt werden.

Sichere E-Mail aus Deutschland:
Die Initiative *E-Mail made in Germany* besteht aus großen deutschen E-Mail Anbietern und propagiert, dass die Daten »verschlüsselt übertragen [werden], sowohl zwischen unseren Nutzern und unseren Rechenzentren als auch untereinander« [*E-Mail made in Germany* 2014]. Dazu wird SSL eingesetzt. Verschleiert wird, dass damit nur die Verbindung vom Nutzer zum E-Mail Anbieter verschlüsselt wird, nicht aber die Nachricht selbst – sie kann vom Anbieter, Behörden, Angreifern auf den E-Mail-Server usw. ohne Aufwand gelesen werden. Der Nutzer wird nicht über die Risiken der angebotenen Sicherheit aufgeklärt.

Im TCP/IP-Referenzmodell werden keinerlei Sicherheitsbestimmungen direkt umgesetzt. Nutzer müssen sich also aktiv um die Sicherheit kümmern. Der unwissende Nutzer kann nicht einschätzen, wie sicher eine Verbindung ist und wie sicher sie für ihn sein sollte. »Ich habe doch nichts zu verbergen«, erscheint so fast als Ausrede dafür, es eben nicht besser zu wissen. Zugleich wird durch Medien und Anbieter oftmals eine *scheinbare* Sicherheit propagiert (vgl. Kasten links), die nicht für jeden direkt identifizierbar ist. Letztlich muss das Ziel sein, dass eine Kommunikation vom Anfang bis zum Ende, d. h. zwischen den beteiligten Endknoten bzw. den Nutzer(systemen), vertraulich, authentifiziert und integriert abläuft. Denn jede Form der (unverschlüsselten) digitalen Kommunikation kann abgehört werden.

2.6.3 Möglichkeiten, um Sicherheit zu erreichen

Über Sicherheitsaspekte und mögliche Strategien zur Umsetzung könnten ganze Bücher gefüllt werden. Im Rahmen dieser Arbeit werden einige wesentliche Ideen und Hinweise dargestellt. Letztlich müssen die unterschiedlichen Schichten jeweils eigene Aspekte der Sicherheitsziele umsetzen, denn beim Routing der Pakete müssen Header von Systemen betrachtet werden können, die von der Nachricht, evtl. der Übertragung selbst, nichts erfahren sollen (vgl. [TANENBAUM, 2003, S. 723]). Die letzten Abschnitte sollten gezeigt haben, dass aus Anwendersicht eine Verbindung dann sicher ist, wenn sie von Endknoten zu Endknoten sicher ist. Emilie möchte, dass ihre Nachrichten zu Lisa so übertragen werden, als wären nur sie beide an der Übertragung beteiligt.

Grundlage sämtlicher Sicherheitsbemühungen ist die Kryptographie (vgl. [ANDERSON, 2008; TANENBAUM, 2003, Kap. 8.1; STEIN, 2008, Kap. 5.6.2]). Sofern verhindert werden soll, dass Dritte eine Nachricht mitlesen können, muss diese verschlüsselt werden. Durch moderne Verschlüsselungsverfahren kann eine ausreichend hohe Sicherheit hergestellt werden. Dabei wird oft neben der Geheimhaltung auch die Authentizität durch entsprechende Zertifikate bzw. Schlüssel sichergestellt. Als Beispiele seien hier PGP[6] zur Verschlüsselung von E-Mails oder SSL[7] zum verschlüsselten Empfang einer Webseite erwähnt. PGP stellt eine Ende-zu-Ende-Verschlüsselung und Authentifizierung sicher und arbeitet unabhängig vom verwendeten Anwendungsprotokoll. SSL stellt eine Möglichkeit dar, die Verbindung zu verschlüsseln und zu authentifizieren.

2.7 Fundamentale Ideen und Netzwerke

Wie in Abschnitt 1.1, S. 1 beschrieben, sollen Kompetenzen identifiziert werden, die Individuen in die Lage versetzen, in der Situation Cyber-Mobbing sinnvoll handeln zu können. Dazu wurden in diesem Abschnitt einige

[6] *Pretty Good Privacy*, `https://de.wikipedia.org/wiki/Pretty_Good_Privacy`, zuletzt betrachtet: 2014-06-20

[7] *Secure Sockets Layer*, `https://de.wikipedia.org/wiki/Transport_Layer_Security`, zuletzt betrachtet: 2014-06-20

fachliche Überlegungen angestellt, um grundlegende Konzepte der Kommunikation in Netzwerken herauszustellen. Anspruch an Kompetenzen ist eine gewisse Zeitinvarianz. Demnach wäre es wenig sinnvoll, Kompetenzen auszubilden, deren Nutzen sich nur auf eine sehr kurze Zeit beschränkt. Zugleich stellt sich die Frage, ob der mögliche Anwendungsbereich der Kompetenzen breit oder sehr speziell ist. Daher erscheint das Konzept der fundamentalen Ideen am besten geeignet, um die angeführten fachlichen Grundlagen auf mögliche Beschreibungsschema und Handlungsdimensionen zu untersuchen.

> »Eine fundamentale Idee bzgl. eines Gegenstandsbereichs (...) ist ein Denk-, Handlungs-, Beschreibungs- oder Erklärungsschema, das
>
> 1. in verschiedenen Gebieten des Bereichs vielfältig anwendbar oder erkennbar ist (*Horizontalkriterium*),
> 2. auf jedem intellektuellen Niveau aufgezeigt und vermittelt werden kann (*Vertikalkriterium*),
> 3. in der historischen Entwicklung des Bereichs deutlich wahrnehmbar ist und längerfristig relevant bleibt (*Zeitkriterium*),
> 4. einen Bezug zu Sprache und Denken des Alltags und der Lebenswelt besitzt (*Sinnkriterium*)« [HUMBERT, 2006, S. 36].

Aus der fachlichen Analyse wurden vier Themenbereiche als wichtig herausgestellt: Topologien, Protokolle, Pakete und Sicherheitsziele. Die technischen bzw. physikalischen Voraussetzungen für die Übertragung von Signalen wurde außen vor gelassen, da die Auswirkungen zum einen unspezifisch für die Netzwerktechnik und zum anderen unbedeutend für das allgemeine Verständnis der Funktionsweise von Netzwerken sind. Anhand der angegebenen Kriterien werden die vier Bereiche kurz unter Aspekten der fundamentalen Ideen untersucht (vgl. [SCHWILL, 1993, S. 10]).

2.7.1 Topologien

Topologien beschreiben und analysieren die geometrische Lage von Verbindungen (vgl. Abschnitt 2.4, S. 8). Verteilte Systeme sind in bestimm-

ten Topologien organisiert, aber auch der Anschluss bzw. die Integration von Hardware in Informatiksysteme werden durch Topologien, z. B. beim Universal Serial Bus (*kurz:* USB), charakterisiert. Sowohl die komplexe Betrachtung (mathematischer) Eigenschaften bis zu simplen Beschreibungen möglicher Wege sind möglich. Topologien durchdringen unseren Alltag in Form von Stationsnetzen von Bussen und Bahnen oder Routenplanern.

2.7.2 Protokolle

In Abschnitt 2.5.1, S. 16 wurde beschrieben, dass die Übertragung von Daten in Netzwerken in einem Schichtenmodell organisiert ist. Ein komplexes Gesamtsystem wird in kleine greifbare Ebenen zerlegt, um es verständlich und anwendbar zu machen.

Die zentrale Idee hinter einem Schichtenmodell, wie es in Netzwerkarchitekturen benutzt wird, könnte Hierarchisierung (n. [ebd., S. 20]) genannt werden. Es ist ein Prinzip, das in unterschiedlichen Bereichen der Informatik, etwa als Sprachhierarchien (Chomsky-Modell), Maschinenmodell oder in der Betriebssystemarchitektur, Anwendung findet. Komplexe Vorgänge in einfache handhabbare Einheiten zu zerlegen ist weder ein neuartiges noch ein kompliziertes Vorgehen. Auch Lexika, die nach Alphabet sortierte Markierungen enthalten, stellen eine Anwendung des Prinzips dar. Aber auch die Klammerung oder Einrückung in Programmiersprachen oder der Aufbau eines Autos in mehreren abhängigen Stationen am Fließband sind Hierarchisierungen. Sowohl das Vertikal-, Zeit- als auch das Sinnkriterium sind somit erfüllt.

Daneben erscheint auch das Prinzip eines Protokolls fundamentalen Charakter zu besitzen. In sämtlichen Bereichen der Informatik müssen Vereinbarungen getroffen werden, wie kommuniziert werden kann. Etwa bei der Interprozesskommunikation, in verteilten Systemen oder in der Kommunikation mit angeschlossener Peripherie. Protokolle gibt es seit den ersten Informatiksystemen und wird es auch in Zukunft in irgendeiner Form immer geben. Letztlich werden auch in der Schule Protokolle umgesetzt. Z. B. müssen die Schüler sich melden, wenn sie etwas sagen wollen und werden daraufhin vom Lehrer aufgerufen. Somit sind Protokolle als fundamentale Idee einzustufen.

2.7.3 Pakete

Pakete sind Datenblöcke, in denen komplexe Datenstrukturen, etwa hierarchisch organisierte Datagramme (vgl. [COMER und DROMS, 2002, Kap. 7]), enthalten sind. Ein großes Paket kann in mehrere kleinere Pakete zerlegt werden. Pakete werden benutzt um Verzeichnisse mit vielen, großen Dateien in eine oder mehrere einzelne Dateien zusammenzufassen. In der Softwaremodellierung mit UML (unified modeling language) umfassen Pakete eine Menge von Modellelementen (vgl. [*Paket (UML)* 2014]). Ein einfaches Prinzip stellt schon die Eimerkette zur Löschung eines Feuers dar. Die große benötigte Menge Wasser wird hier auf mehrere Pakete bzw. Eimer aufgeteilt. Komplexer ist dagegen die Betrachtung von IP-Paketen.

2.7.4 Sicherheitsziele

In [FREISCHLAD, 2010, S. 36ff] wurde die Tauglichkeit als fundamentale Idee der, auch in dieser Arbeit angegebenen Sicherheitsziele, ausführlich bestätigt. Daher soll ein grober Überblick genügen.

Sicherheitskonzepte werden nicht nur in Netzwerken, sondern auch bei der Architektur von Betriebssystemen benötigt, damit verschiedene Prozesse und Benutzer *quasi*-gleichzeitig kommunizieren können. Aber auch beim Anschluss von Peripherie sind Sicherheitsziele wichtig, um etwa bei mehreren per USB angeschlossenen Speichermedien Schreib- und Lesezugriffe zu sichern. Dass die Haustür abgeschlossen werden muss oder gar Alarmanlagen eingebaut werden, um Besitz und Privatsphäre zu schützen, ist heute jedem bewusst. Autos erhalten komplexe Sicherheitssysteme, um die Insassen zu schützen. In Zukunft werden immer aufwendigere Sicherheitsvorkehrungen entstehen, so dass Autos möglicherweise bald ohne Fahrer sicher fahren können (vgl. [SCHWAN, 2014]). Die Schutzziele erscheinen sowohl im Anforderungsniveau breit als auch sinnhaft und zeitlich invariant.

2.8 Fazit

Die fachliche Analyse der Kommunikation in Netzwerken hat zentrale Konzepte, wie Topologie, Protokolle, Pakete und Sicherheit, herausgestellt. Mithilfe der Kriterien zu fundamentalen Ideen konnten die fachlichen Konzepte auf ihre Tauglichkeit als Erklärungs- und Beschreibungsschema hin untersucht werden. Deutlich wird so, dass entgegen des oft gefühlt nur sehr kurzlebigen Geschäfts von Angeboten im Internet, Konzepte für die Kommunikation in Netzwerken keine neuartigen Ideen sind. Gewissermaßen kann somit nicht von der *Entdeckung des Internets* gesprochen werden. Die benutzten Konzepte und Technologien stellen praktisch alten Wein in neuen Flaschen dar (vgl. [HELLIGE, 2006]).

Damit zeigt sich aber auch ein wichtiger Schritt in der Findung von informatischen Kompetenzen zum Umgang mit Cyber-Mobbing. Mobbing kann nicht nur in der Schule, sondern das ganze Leben über auftreten. Somit müssen die Kompetenzen einen unspezifischen Transfer auf neue Situationen und Problemstellungen fördern. Allgemeine Denkweisen, Prinzipien usw. können, sofern sie etwa den Kriterien fundamentaler Ideen genügen, einen solchen Transfer ermöglichen (vgl. [SCHWILL, 1993, S. 2f]). Die hier angegebenen fachlichen Konzepte können dies leisten – vor allem da sie ein Verständnis mit einer sehr langen Lebensdauer liefern, das nicht unnütz ist, sobald die Firma eines bestimmten Angebots Konkurs anmeldet.

Bisher wurden die konkreten Anwendungsdienste und Angebote nicht weiter untersucht, da Konzepte zum Verständnis eher der Softwaretechnik zuzuschreiben wären und daher den fachlichen Rahmen sprengen würden. Im weiteren Verlauf dieser Arbeit muss nun gezeigt werden, dass aus den fundamentalen Ideen der Kommunikation in Netzwerken auch wirkliche Handlungsschema bzw. -dimensionen in der Situation Cyber-Mobbing entstehen. Dafür sollten auch die genutzten Angebote hinsichtlich der erarbeiteten Konzepte genauer betrachtet werden.

Offen bleibt damit die explizite Betrachtung des gesamten Protokollstapels. Im weiteren Verlauf dieser Arbeit, wird die Anwendungsschicht vor allem hinsichtlich der Auswirkungen für die Gesellschaft bzw. die handelnden Menschen untersucht. Um den Rahmen dieser Arbeit nicht zu sprengen, wird auf die detaillierte Diskussion der Zusammenhänge zwischen konkreten Diensten bzw. Angeboten und den in diesem Abschnitt erarbeiteten

Fachkonzepten verzichtet. Weitere Hinweise können der jeweils angegebenen Fachliteratur entnommen werden.

http://www.springer.com/978-3-658-14378-7

Kompetenzen in der Informatik zur Prävention von Cybermobbing
Chancen und Wege des Informatikunterrichts an Schulen
Hilbig, A.
2016, XI, 77 S. 7 Abb., Softcover
ISBN: 978-3-658-14378-7