Interreg

EUROPÄISCHE UNION

Österreich-Tschechische Republik

Europäischer Fonds für regionale Entwicklung

INFORMATIK

Netzwerke

UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

VŠTE

EUROPÄISCHE UNION

Inhalt

1. Grundbegriffe 3
1.1. Wozu braucht man ein Computernetzwerk? 5
2. Netzwerktopologie 7
2.1. Computernetzwerke und ihre Dienste 8
2.2. Netzwerktopologien 8
3. Was ist das Internet? 10
3.1. Die Entstehungsgeschichte des Internets 10
3.2. Die Entwicklung des Internets 11
3.3. Wozu braucht man das Internet? 12
3.4. Ethernet 12
4. Standardisierung v. Computernetzwerken, TCP/IP Stack 15
4.1. Standardisierung von Computernetzwerken 15
4.2. Grundbegriffe RM OSI 16
4.3. ISO/OSI Referenzmodell 17
4.3.1. Anwendungsschicht 18
4.3.2. Darstellungsschicht 18
4.3.3. Sitzungsschicht 18
4.3.4. Transportschicht 19
4.3.5. Netzwerkschicht 19
4.3.6. Sicherungsschicht 19
4.3.7. Bitübertragungsschicht 20
4.4. TCP/IP Modell 20
4.5. Architektur von TCP/IP-Protokollen 21
4.6. Architektur kommunizierender Systeme 22
5. ISO/OSI Modell, ausgewählten Protokolle 23
5.1. Computernetzwerke - ISO/OSI-Modell 23
5.2. ISO/OSI-Referenzmodell: Sieben Schichten 25
6. Drahtlose Kommunikationstechnologien 28
6.1. Eigenschaften drahtloser Netzwerke 30
6.1.1. Geschwindigkeit 30
6.1.2. Sicherheit 30

6.1.3. Anwendung 32
7. Virtuelle Netzwerke (VLAN). 33
7.1. Wozu braucht man ein VLAN? 33
7.2. Die größten Vorteile von VLAN 37
7.3. Grundsätze der VLAN-Kommunikation 38
8. URL, X/HTML, HTTP 40
8.1. Arten von URLs 40
8.2. Die Bedeutung der URL-Gestaltung 41
8.3. XHTML 44
8.4. HTTP 45
9. Routingprotokolle 49
9.1. Routing: Technische Begriffe 50
10. Sicherheit und Verschlüsselung 53
10.1. Netzwerksicherheit 53
10.2. Firewall 54
10.3. Verschlüsselung 54
11. Peer-to-Peer Netzwerke 59
11.1. Generationen von P2P-Netzwerken 60
11.2. Filehosting 62
12. Anonymität im Internet 64
12.1. Technologien zum Schutz der Privatsphäre 65
12.2. Grundprinzipien zur Wahrung der Anonymität 66
12.3. TOR: Total anonymes Internet 68
13. Angriff und Verteidigung im Internet 74
13.1. Angriff und Verteidigung des PCs 74
13.1.1. Angriff 74
13.1.2. Schutz 76
13.2. Gefährliches Netzwerk: Angriffe abwehren 78
14. Literatur 84

1. GRUNDBEGRIFFE

In diesem Teil werden all jene Grundbegriffe umfassend erklärt, auf welche Studierende im Bereich der Computernetzwerke stoßen könnten. Es ist an dieser Stelle jedoch wichtig festzuhalten, dass die hier zu findenden Anmerkungen nicht als präzise Definition betrachtet werden können: Sie beziehen sich eher auf ein komplexes Feld mit vielen erwähnenswerten Ausnahmen von der Regel. Nichtsdestotrotz sollen Studierende zumindest eine allgemeine Vorstellung davon haben, was man unter diesen Schlagworten versteht und in der Lage sein, diese effizient zu verwenden.

Client: Darunter versteht man einen Computer, welcher an ein Netzwerk angeschlossen ist. Er hat in der Regel keinen privilegierten Status und seine Möglichkeiten sind jenen von anderen Clients sehr ähnlich. Dieser Begriff begegnet einem auch bei Kennzeichnungssoftware, welche mit dem Server kommuniziert und – auf diese Weise – einen Nutzer mit wesentlichen Diensten (FTP Client, E-Mail-Client usw.) versorgt.

Server: Dieser Begriff bezieht sich auf einen Computer mit einem privilegierten Status im Netzwerk. Von ihm wird verlangt, Clients mit wesentlichen Diensten oder Funktionen zu versorgen. Dazu gehören z.B. die effektive Kommunikation von Clients, die Domainnamen-Überführung in IP-Adressen (DNS), Internetverbindung, Drucken, Filesharing usw. In Beziehung zu einem anderen Server kann ein Server jedoch als Client betrachtet werden. Hierbei handelt es sich in der Regel um speziell konstruierte Computer (spezieller Prozessor, Disk-Matrix usw.).

Router: Dieses Gerät stellt die Paketweiterleitung sicher. Es bindet ein Netzwerkelement, dessen Umgebung es im Detail kennt, mit ein und stellt gleichzeitig sicher, dass die Paketweiterleitung in die richtige Richtung erfolgt. Setzt man ein Paket mit einem Brief gleich, so übernimmt der Router die Rolle des Postdienstes. Doch sein Einsatz reicht noch weiter: Ein Router garantiert qualitativ hochwertige Dienste und stellt TTL sicher (ein Parameter, der die Lebensdauer von Paketen begrenzt, damit sich ein verlorenes Paket nicht für immer im Umlauf befindet). Darüber hinaus sollte er sorgfältig seine Umgebungen erkunden und Netzwerkveränderungen feststellen. Gleichzeitig berechnet er den besten Weg zu weiteren Netzknoten.

Packet: Dies entspricht einem festen Datensatz, welcher über das Netzwerk versendet wird. Daten werden in der Regel nicht (fast nie) als ununterbrochener Informationsfluss gesendet, sondern als Datensätze, sprich Pakete. Dieses aufwändige System macht es sicherer, gewährleistet richtiges Routing sowie die effektive Nutzung der Netzwerkkapazität. Obwohl das Paket eine starre Struktur hat, enthält es in der Regel die Adresse des Senders und Empfängers, Informationen über das Protokoll, Daten oder andere Hilfsinformationen.

Netzwerkkarte: Dies ist eine Hardwarekomponente (heutzutage für gewöhnlich fest im Motherboard verbaut), welche die Netzwerkverbindung sicherstellt. Darin enthaltene Informationen werden in Pakete umgewandelt und Pakete in Daten. Die Karte kann ein spezifisches Datentransferprotokoll ausführen (in der Regel Ethernet) und enthält auch einen Kabelanschluss (Twisted-Pair-, Glasfaser-, Koaxial-Kabel). Darüber hinaus enthält die Karte eine spezifische MAC-Adresse, welche weltweit einzigartig ist und zur Identifikation des Computers im Netzwerk dient oder alternativ eine lokale Adresse erzeugt.

Schnittstelle (Port): Diese hat eine Nummer zwischen 0 und 65535, welche eine Anwendung identifiziert, die aktuell als Kommunikationsmittel verwendet wird. Einzelne Anwendungen werden innerhalb des TCP- oder UDP-Protokolls identifiziert. Ports ermöglichen eine Anwendungswartung, stellen (bis zu einem gewissen Grad) die Qualität der Services sicher usw. Es gibt in der Tat feste Anschlussnummern, SMTP hat zB die 25, POP3 die 110, HTTP die 80 oder FTP die 21. Zugleich können sich, auch wenn es unüblich ist, Nutzer oder Anwendungen auf eine andere Port-Nummer verständigen.

Medium: Dieses stellt die physische Umgebung dar, in der die Netzwerkkommunikation ausgeführt wird. Dazu gehören LED-Medien, sprich klassische Kabel (Glasfaser-, Metall-, Twisted-Pair-Kabel) oder Wellenlängen-Medien (Luft, Vakuum), welche Technologien wie WiFi oder GSM nutzen.

Protokoll: Hierbei handelt es sich um eine formelle Sprache, welche die Art der Kommunikation festlegt (IP, TCP, and IMAP4). Es beschreibt genau das Paket, sprich die Geschwindigkeit, mit der es gesendet werden soll. Darüber hinaus definiert es die Sicherheitselemente, korrigiert Fehler usw. Fast jede Schicht des ISO-OSI-Modells enthält seine eigene Gruppe von Protokollen. Diese sind in der Regel an eine Ebene gebunden.

Netzwerkweiche (Switch): Dies ist ein aktives Netzwerkelement, welches Netzwerkteile verbindet. Anders al seine Brücke erlaubt es ein Verteiler, mehr als zwei Netzwerkschleifen miteinander zu verbinden. Kleinere Netzwerkteile haben einen besseren Zugang zum Medium, wodurch eine höhere Übertragungsgeschwindigkeit und Netzwerkauslastung sichergestellt wird.

Repeater: Dieser Begriff bezeichnet ein einfaches Gerät, welches die Signalübertragung über weitere Strecken sicherstellt. Es befindet sich in einem bestimmten Abstand zum Transmitter und verstärkt das ankommende Signal. Dadurch arbeitet es direkt auf der physischen Ebene.

1.1. Wozu braucht man ein Computernetzwerk?

Unternehmen installieren Computernetzwerke zumeist deshalb, weil sie darüber Ressourcen teilen und eine direkte Kommunikation ermöglichen möchten. Zu den Ressourcen gehören Daten, Anwendungen und periphere Geräte, zB externe Laufwerke, Drucker oder Modems. Die direkte Kommunikation umfasst das Senden von Nachrichten, das Antworten darauf oder E-Mail-Dienste.

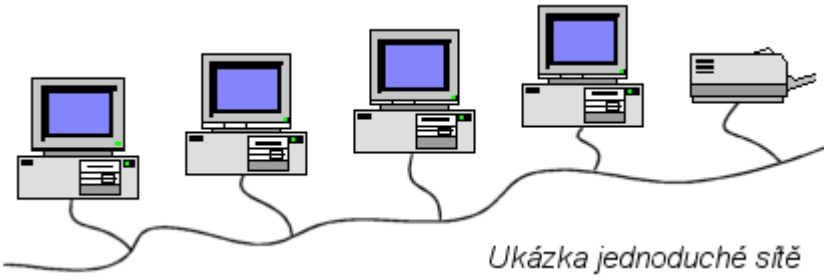


Abb.: Illustration eines einfachen Netzwerks

Computernetzwerk ist ein allgemeiner Begriff für technische Geräte, mit deren Hilfe eine Verbindung und ein Datenaustausch zwischen Computern ermöglicht wird. Darüber hinaus ermöglicht es nutzern, regelkonform zu kommunizieren. Der wichtigste Grund für eine Netzwerkverbindung ist das Teilen von Informationen und technischen Geräten.

Abb.: Eine sternförmige Netzwerkverbindung

Nach ihrer Weitläufigkeit unterscheidet man 4 Computernetzwerke

- PAN (Personal Area Network): Dies ist ein Netzwerk, welches ein sehr kleines Gebiet abdeckt (kleiner als die LAN-Zone). Zum Netzwerk gehören Kommunikationsgeräte wie Handys oder Laptops.

- LAN (Local Area Network): Hierbei handelt es sich um ein lokales Netzwerk, welches ein kleines Gebiet abdeckt, welches zwar größer als die PAN-, aber kleiner als die MAN-Zone ist.

- MAN (Metropolitan Area Network): Dieses Netzwerk ist größer als die LAN-, aber kleiner als die WAN-Zone.

- WAN (Wide Area Network): Dieses Netzwerk deckt ein riesiges Gebiet ab, welches deutlich größer als die MAN-Zone ist.

- VLAN: Darunter versteht man ein virtuelles LAN (Netzwerk). Es handelt sich um ein virtuelles Netzwerk, welches sich innerhalb des LAN-Netzwerks bildet und in einer Hardwarekomponente (Kabel) betrieben wird. VLAN funktioniert auf der Grundlage der Interpretation von Daten, welche über das Netzwerk übertragen werden. Die Daten werden entsprechend des zugehörigen Netzwerks interpretiert.

2. NETZWERKTOPOLOGIE

Die Netzwerktopologie beschreibt die physikalische Verbindung. Genauer gesagt ist es möglich, zwischen einer logischen und einer physikalischen Computerverbindung zu unterscheiden.

Ring: Dieser Begriff bezieht sich auf eine zirkuläre Verbindung von Computern. Hierbei ist ein Computer immer mit zwei anderen verbunden. Der größte Vorteil dieses Modells ist, dass das Netzwerk aufrechterhalten werden kann (vorausgesetzt es ist ein Duplex), wenn ein Element ausfällt. Darüber hinaus kommunizieren die sich am nächsten befindenden Computer (im LAN-Netzwerk) am öftesten miteinander.

Mesh: Hierbei handelt es sich wahrscheinlich um die am seltensten verwendete Topologie. In der Tat gibt es hier keine Grundregeln, weshalb es ad-hoc über sich progressiv verbindende Computer gebildet wird. Auf der anderen Seite ist ihre Beschreibung ziemlich interessant, da sie sehr einfach ist. Logisch betrachtet kann man sagen, dass es sich bei Mesh um ein Internet als Ganzes handelt.

Stern: Dieses Verbindungsmodell ist das gängigste: Seine einzelnen Stationen sind mit einem zentralen Punkt verbunden (zB einem Server), welcher die gesamte Kommunikation übernimmt. Ein großer Vorteil ist sein effektives Management und seine klare Richtung. Der Schwachpunkt ist jedoch der Server.

Baum: Dieser Begriff bezieht sich auf eine andere häufig verwendete Topologie. Hierbei handelt es sich um eine komplexe Computerstruktur, die der Struktur eines mathematischen Baums entspricht. Dadurch können einzelne Computer (sofern es sich nicht um End-zu-End oder Root-Computer handelt) zugleich die Rolle des Servers und des Clients übernehmen.

Bus: Dies ist ein Modell, in welchem die Stationen progressiv an ein Medium angeschlossen werden. Daher hat man es hier mit dem Konzept eines gemeinsamen Mediums zu tun.

Klarerweise gibt es noch eine Reihe weiterer wichtiger Topologien: lineare, wechselseitige und den Extremfall der Punkt-zu-Punkt-Verbindungen. Für gewöhnlich sind Computernetzwerke jedoch irgendwo dazwischen angesiedelt.

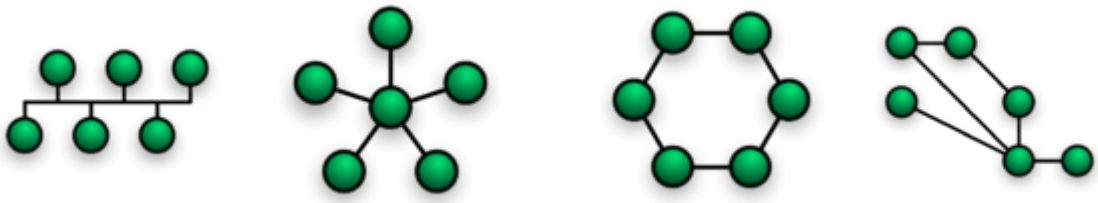
2.1. Computernetzwerke und ihre Dienste

Ein Computernetzwerk ist ein allgemeiner Begriff für technische Geräte, welche eine Verbindung und Datenübertragung ermöglichen. Ebenso erlauben sie Nutzern eine regelkonforme Kommunikation. Der Hauptzweck von Netzwerkverbindungen ist das Teilen von Infos und technischen Geräten.

Abb.: Computernetzwerk

2.2. Netzwerktopologien

Der Begriff Topologie bezeichnet die Vernetzung von Computern. Darüber hinaus enthält er Informationen über die spezifische Anordnung der miteinander verbundenen Computer und deren Kommunikation. Mögliche Vernetzungsmethoden sind nachstehend abgebildet:



Bus-Topologie | Stern-Topologie | Ring-Topologie | Unbegrenzte Topologie

Abb.: Topologien: Mögliche Formen von Computernetzwerken

Die Verbindungen der **Bus-Topologie** kommt über ein Übertragungsmedium zustande, welches Bus genannt wird. Mit diesem sind alle Endgeräte, z.B. Netzwerkknoten, verbunden.

Die **Stern-Topologie** bezieht sich auf eine sternförmige Netzwerkverbindung. Es handelt sich hierbei um die häufigste Methode, um Computer zu verbinden. Sie basiert auf einem Computer in der Mitte, welcher auch Zentralcomputer genannt wird. Dieser ist mit den ihn umgebenden Computern vernetzt. Man kann sich vorstellen, dass einer oder mehrere Ende-zu-Ende-Computer durch den Zentralcomputer ersetzt werden. Daher wächst das gesamte Netzwerk progressiv.

Als **Ring-Topologie** bezeichnet man eine Verbindung, bei welcher ein Netzwerkknoten mit zwei anderen Netzwerkknoten in Form eines Rings verknüpft ist. Diese Topologie ist allerdings nicht allzu schnell, da eine große Anzahl an Netzwerkknoten verhindert, dass Daten schnell an den Zielrechner übertragen werden. Darüber hinaus ist in dem Fall, dass einer der Netzwerkknoten nicht funktioniert, ist kein Datentransfer möglich. Somit bricht das gesamte Netzwerk zusammen. Diese Art der Verbindung wird heutzutage kaum noch verwendet, da die Stern-Topologie deutlich zuverlässiger ist. Andererseits sind die Kosten für den Aufbau eines solchen Netzwerks geringer.

3.WAS IST DAS INTERNET?

Das Internet ist ein globales Netzwerk, welches einem gewöhnlichen Computernetzwerk sehr ähnlich ist. Computer werden miteinander verbunden, wodurch sie in die Lage versetzt werden, miteinander zu kommunizieren und Informationen zu teilen. Das Internet verbindet schon bestehende Netzwerke über eine kohärente Struktur und Distribution miteinander.

Das Internet kann auch als ein Computersystem bezeichnet werden, welches Informationen und Netzwerke enthält, welche uns mit bestimmten Informationen versorgen.

Computer innerhalb des Internets übernehmen entweder die Rolle von Clients oder Servern. Server stellen Internetdienste zur Verfügung, von welchen Clients in der Folge Gebrauch machen. Darüber hinaus stellen Internetdienste auf Anfrage den Datentransfer zu einem Client sicher.

3.1. Die Entstehungsgeschichte des Internets

Während des Kalten Kriegs benötigten die USA ein funktionelles Managementsystem, welches in der Lage sein sollte, die wichtigsten wissenschaftlichen, strategischen und Regierungscomputer (Länder, Militärbasen usw.) miteinander zu verknüpfen. Die Hauptanforderung war es, ein starkes Netzwerk aufzubauen, welches selbst dann, wenn einige Netzwerkknoten ausfielen, weiter aufrecht bleiben und zumindest eine teilweise Kommunikation sicherstellen konnte.

In den 1960er-Jahren wurde die RAND Corporation Company damit beauftragt, eine Lösung zu finden, die es ermöglichte, dass Computer auch nach einem Atomkrieg reibungslos liefen. Die Haupt-aufgabe bestand darin, ein System zu entwerfen, welches selbst nach einer möglichen Zerstörung ihrer Teile stabil funktionieren würde.

Im Jahr 1964 stellte ebendiese Firma eine umfassende Lösung vor, welche auf zwei zentralen Prinzipien beruhte:

- Das Netzwerk enthält keine zentrale Komponente
- Das Netzwerk läuft selbst dann, wenn einige seiner Teile außer Betrieb sind

In Anbetracht dieser Umstände kann man also sagen, dass die US-amerikanische Armee, sprich das Pentagon, das Internet erschaffen hat. Im Jahr 2010 wurden bereits zwei Milliarden aktive Internetnutzer gezählt.

3.2. Die Entwicklung des Internets

Phase Null

Die Phase Null begann, als die US-amerikanische Armee eine effektive Kommunikation zwischen einzelnen Regierungsabteilungen im Falle eines Atomkriegs in der Zeit des Kalten Kriegs aufbauen musste. Das US-Verteidigungsabteilung, sprich die ARPA (Agentur für fortgeschrittene Forschungs-projekte), richtete das ARPANET-Netzwerk ein und schaffte es, dieses Projekt zu finanzieren.

Erste Phase

In der ersten Phase konnte man auf die in späterer Folge mächtigsten Computer zugreifen. Dies waren hauptsächlich jene der Universitäten in den USA. Im Spätherbst des Jahres 1969 wurden die ersten Netzwerkknoten des ARPANET-Netzwerks an den Universitäten in Betrieb genommen. Das Hauptziel war es, nicht nur einen Computer, sondern das gesamte Netzwerk einzubinden. Die Entwicklung fand in allen möglichen Organisationen statt. In der Folge nahmen auch lokale Computer-Netzwerke ihren Betrieb auf. Zu Beginn der 1980er verzeichnete das ARPANET eine rasante Entwicklung, welche auch in anderen Netzwerken stattfand. In der Folge wurden Netzwerke wie Usenet oder BITnet geschaffen. Letztendlich wurden alle Netzwerke an das ARPANET angeschlossen. 1987 waren mehr als 10.000 Netzwerkknoten registriert, zwei Jahre später waren es bereits zehnmal mehr.

In den 80er- und 90er-Jahren wurden Dienste erweitert, mit welchen die Menschen von heute vertraut sind und welche sie nutzen. Diese waren hauptsächlich E-Mail (1971), telnet (1972), TCP (1974) und dessen Updates TCP/IP (1978), DNS (1983) und dessen Start im Jahr 1984. Im Jahr 1980 entschied sich das Pentagon dafür, TCP/IP-Protokolle zu den bevorzugten Protokollen für das Verteidigungsministerium wären. Zwei Jahre später mussten alle Computer, welche an das ARPANET-Netzwerk angeschlossen waren, auf TCP/IP-Protokolle umstellen. Dadurch wurde das ARPANET zu einem Netzwerk und einem Konglomerat aus nebeneinander existierenden und sich neu etablierenden Netzwerken. Allmählich begann sich das Internet abzuzeichnen.

Zweite Phase

Die zweite Phase erstreckt sich über den Zeitraum der Internetentwicklung von 1983 bis 1992. Diese Periode war gekennzeichnet durch ein dramatisches Wachstum des Internets und hauptsächlich durch dessen Verbreitung über die Grenzen Amerikas hinaus. Das ARPANET wurde mit anderen Netzwerken wie dem NFSNET, EUNET, EARN, JUNET usw. verknüpft.

Im November 1983 wurde das DNS Domainsystem eingeführt, welches numerischen Adressen die Zuordnung von Domainnamen erlaubte. Im Jahr 1989 wurde das WWW (World Wide Web) eingeführt, welches in späterer Folge zu einem integralen Bestandteil des In-

wurde. Im Jahr 1990 wurde das ARPANET stillgelegt und in der Folge eliminiert. Von da an war das NFSNET das zentrale Internetnetzwerk. Im Jahr 1991 wurde die Tschechische Republik an das Internet angeschlossen. 1993 begann man mit der zivilen Nutzung.

3.3. Wozu braucht man das Internet?

Dank des Internets können dessen Nutzer eine Reihe von Diensten verwenden. Diese Dienste werden von Computerprogrammen zur Verfügung gestellt, welche miteinander via Protokoll kommunizieren. Zu den grundlegenden Internetdiensten gehören mitunter:

- **WWW:** Ein System von Webseiten, welches von einem Browser angezeigt wird. Es verwendet HTTP/HTTPS-Protokolle.
- **E-Mail:** elektronische Post
- Versenden von Nachrichten via **SMTP-Protokoll**
- Erhalten von Nachrichten via **POP3- und IMAP-Protokoll**
- **IM (Instant messaging):** Echtzeit-Kommunikation online via ICQ, Jabber, Skype
- **FTP:** Datenübertragung
- **DNS:** Domainnamensystem, welches zum Zwecke besserer Erinnerung eingesetzt wird

Darüber hinaus könnte man eine Reihe weiterer Protokolle erwähnen, zB zum Datenteilen (NFS), Protokolle zum Verbinden zu einem fernsteuerbaren Computer (telnet, SSH, VNC) usw.

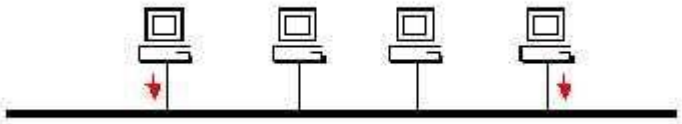
3.4. Ethernet

Ethernet ist eine Technologie für Computernetzwerke. Es repräsentiert ein Set von Technologien, deren Hauptzweck die Datenübertragung in LAN-Netzwerken ist. Die meisten Ethernet-Versionen sind den Standards des IEEE (Institute of Electrical and Electronics Engineers) unterworfen. Ethernet wird über die erste (Bitübertragungs-) und zweite (Sicherungs-) Schicht des ISO/OSI-Referenzmodells implementiert. Darüber hinaus verwendet es hauptsächlich Twisted-Pair- und Glasfasterkabel als Übertragungsmedium: Die ersten Versionen verwendeten hierzu noch Koaxial-Kabel. Der nächste integrale Bestandteil ist der RJ_45 Connector. Es gibt verschiedene Arten von Ethernet, je nachdem, welches Kabel und welche Übertragungsgeschwindigkeit zum Einsatz kommen. Die Übertragungs-geschwindigkeit variiert zwischen 10 Mbit/s und 100 Gbit/s.

Heutzutage ist Ethernet die am häufigsten verwendete Netzwerktechnologie. Diese Technologie basiert auf einem äußerst einfachen Prinzip, welches CSMA/CD genannt wird – und zwar unabhängig davon, ob es sich um ein gewöhnliches 10 Megabit Ethernet oder eine schnellere Variante davon handelt (Fast und Gigabit Ethernet).

Ein gut strukturiertes Kabelsystem kann diverse Arten von Netzwerktechnologien verwenden, welche auf verschiedenen Arten von Übertragungsmethoden basieren, z.B. Ethernet, Token Ring, CDDI, ATM usw.

Bei **CSMA** (Carrier Sense Multiple Access) handelt es sich um eine Station, welche bereit ist, Daten und zu übertragen und "überprüft", ob das Übertragungsmedium (Kabel) von einer anderen Station verwendet wird. In so einem Fall versucht die Station, später darauf zuzugreifen, bis das Medium frei ist. Ab dem Moment, ab dem das Medium frei ist, beginnt die Station mit der Datenübertragung.



CD (Collision Detection) bezieht sich auf eine Station, welche während der Übertragung überwacht, ob das Medium ein Signal anzeigt, welches mit den Übertragungsebenen übereinstimmt (sprich, um nicht Signal 1 zu übertragen, wenn gerade Signal 0 übertragen wird). Diese Art der komplexen Signal-Interaktion wird Collision genannt. Im Falle einer **Detection** sendet die Collision-Station ein JAM-Signal aus und beide (alle) Stationen erzeugen zum selben Zeitpunkt der Übertragung einen zufälligen Zeitwert, nach welchem sie versuchen werden, die Übertragung zu wiederholen.

Tatsächlich war diese Effektivität verantwortlich dafür, dass die Preise von AC-Adaptern und aktiven Elementen fielen und sich Ethernet in der Folge merklich verbreitete. Gleichzeitig brachte die Effektivität einer solchen Lösung einen gravierenden Nachteil mit sich: Durch die steigende Zahl der Netzwerkknoten erhöhte sich gleichzeitig die Zahl der Collisions. Dadurch verringert sich die theoretische Durchsatzleistung des Netzwerks. Das Knoten-Set, durch welches die gewöhnliche Aktivität eine Collision auslösen kann, wird Collision Domain genannt. Logisch kann daraus abgeleitet werden, dass die **Collision Domain** so klein wie möglich sein sollte. Angelegte aktive Elemente haben eine unterschiedliche Beziehung zur Collision Domain: Auf der einen Seite erweitern mache davon die Collision Domain, auf der anderen Seite trennen manche diese ab. Deshalb kann man durch sorgfältige Auswahl der aktiven Elemente die Durchsatzleistung des Netzwerks steuern.

Zusätzlich wurde, abgesehen von der Collision Domain, der Begriff **Broadcast Domain** eingeführt. Das Computernetzwerk enthält zwei Arten von Paketen: Unicasts und Non-Unicasts. Der Begriff Unicasts bezieht sich auf Pakete mit einem bestimmten Adressaten, welcher von der Netzwerkadresse zur Verfügung gestellt wird. Andererseits neigen Non-Unicasts dazu, eine Gruppenadresse zu verwenden und sind entweder für alle Netzwerknutzer (Broadcasts) oder eine ausgewählte Nutzergruppe (Multicasts). Das Hauptproblem ist, dass ein Computer sich mit Non-Unicast beschäftigten muss, auch wenn er darauf nicht ausgelegt ist. Deshalb erhöht sich gleichzeitig mit der Zahl der Netzwerkknoten

durch eine große Zahl an Non-Unicasts auch die Broadcast Domain. Aus diesem Grund ist es notwendig, die Größe der Broadcast Domain in vernünftigen Grenzen zu halten. Angelegte aktive Elemente haben eine unterschiedliche Beziehung zur Broadcast Domain. Folglich kann durch deren sorgfältige Auswahl die Durchsatzleistung des Netzwerks kontrolliert werden.

Paketformat

Wie zuvor beschrieben wurde, werden alle Ethernet-Geschwindigkeitsmodifikationen mit derselben Kommunikationsmethode CSMA/CD erreicht. Sie nutzen allerdings auch dieselbe Paketgröße und dasselbe Paketformat. Das Ethernetpaket ist auf der ersten und zweiten OSI-Schicht definiert.

4. STANDARDISIERUNG V. COMPUTER-NETZWERKEN, TCP/IP STACK

4.1. Standardisierung von Computernetzwerken

Zur Kernstrategie führender Hersteller gehörte das Ausarbeiten und Warten von Spezifikationen, welche genau mit den Produkten der Firmenkunden kompatibel sind. Das größte Manko dieser Computernetzwerke, welche als homogene oder geschlossene Systeme bezeichnet wurden, bestand darin, sich sowohl an die Hersteller von technischer Geräte als auch die Hersteller von Software anzupassen. An dieser Stelle werden ein paar firmeneigene Protokolle genannt: DECnet von DEC, SNA (Systemnetzwerkarchitektur von IBM), SPX/IPX (Sequenzierter/Internet-Paketaustausch von Novell). Im Gegensatz zu diesen geschlossenen Systemen beziehen sich offene oder heterogene Systeme auf Computersysteme, welche in Einklang mit bewährten internationalen Standards entwickelt wurden und von mehreren unabhängigen Produzenten gekauft werden können. Die Umsetzung offener Systeme erlaubt den Programmen, welche in lokalen oder ferngesteuerten Netzwerksystemen zum Einsatz kommen, eng zusammenzuarbeiten und ermöglicht eine einheitliche Kommunikation zwischen den Benutzern der Anwendungen.

Der Begriff OSI (Open Systems Interconnection) betrifft die technische Ausstattung und Computernetzwerksoftware. Im Bereich der Computernetzwerke sind die internationalen Organisationen CCITT (Comité Consultatif International de Télégraphique et Téléphonique als eine der drei zentralen Komitees der International Telecommunications Union ITU) und ISO (International Organzisation for Standardization) die wichtigsten. Sie beschäftigten sich damit, geeignete Standards einzuführen. In der Tat sind Regierungsinstitute oder Organisationen, welche in den einzelnen Mitgliedsländern für die Telekommunikation verantwortlich sind, die wichtigsten Mitglieder der CCITT. Die CCITT gibt detaillierte Empfehlungen heraus, welche nach einer grundsätzlichen Genehmigung von der ITU zu internationalen Standards werden. Im Gegensatz zur CCITT ist die ISO eine freiwillige nichtstaatliche Organisation, dessen Mitglieder Standardisierungsinstitute sind. Eine weitere wichtige Organisation ist die IEEE, bei welcher es sich um eine prestigeträchtige amerikanische Vereinigung von Elektro- und Elektronik-Ingenieuren handelt. Diese Vereinigung gibt Zeitschriften heraus, halt Konferenzen ab und bildet eine professionelle Körperschaft, welche professionelle Standards einführt. Die Standard-gruppe IEEE 802 ist im Bereich der lokalen Computernetzwerke erwähnenswert. Im Jahr 1979 übernahm die ISO einen Standard namens Reference Model of Open Systems Interconnection (RM OSI).

Netzwerkkommunikation

Zu den Hauptaufgaben eines Netzwerks gehört die Datenübertragung von einem Computer zu einem anderen. Dieses komplexe Unterfangen kann in die folgenden Schritte unterteilt werden:

- Datenüberprüfung
- Aufteilen der Daten in nützliche Datenbanken
- Versorgen jeder Datenbank mit nützlicher Information (Quelle und Ziel)
- Bereitstellen relevanter Informationen über zeitliche Abstimmung und Fehlersuche
- Übermitteln von Daten an ein Netzwerk und Versenden dieser an einen geeigneten Ort

4.2. Grundbegriffe RM OSI

Eine **Schicht** ist durch ihre nutzbaren Funktionen genau definiert. Jede Schicht, mit Ausnahme der obersten und untersten, verbindet die jeweils darunter- und darüberliegende Schicht über eine Schnittstelle miteinander. Die oberste Schicht bindet den Umsetzungsprozess über eine Schnittstelle an. Die unterste Schicht bindet zudem über eine Schnittstelle das physikalische Medium an.

Eine Entität ist ein Objekt, welches effektiv in einer bestimmten Schicht arbeitet. Der Begriff bezieht sich für gewöhnlich auf eine Programmgruppe. Zu den unteren Ebenen gehört die Hardware (I/O Port). Der unmittelbare Bereitsteller bzw. Nutzer eines Dienstes beziehen sich nicht auf eine Schicht, sondern auf eine bestimmte Entität einer Schicht.

Zu einem **Protokoll** gehören Entitäten in denselben Schichten verschiedener offener Systeme. Sie **kommunizieren** miteinander.
Der Begriff Service bezieht sich auf Entitäten einer bestimmten Schicht, welche dessen Funktion ausführen. Darüber hinaus stellen sie die höhere Schicht mit den geeigneten Diensten zur Verfügung. Um diese Funktionen ausführen zu können, verwenden sie Dienste aus der direkt darunter befindlichen Schicht. Einzelne Dienste werden von Service Access Points (SAP) angeboten, welche über ihre Adressen identifiziert werden. Diese Dienste lassen sich wie folgt einteilen:

- **Verbindungsorientierte Services:** Zwei Entitäten auf denselben Ebenen müssen zuerst eine Verbindung herstellen, bevor eine direkte Kommunikation gestartet werden kann. Nach dem erfolgreichen Zustandekommen einer Verbindung verschickt der Sender eine Nachricht und der Empfänger erhält diese. Dieser Service ist vergleichbar mit einer Telefonverbindung.

- **Verbindungslose Dienste** setzen kein Zustandekommen einer starken Verbindung zwischen einem Sender und einem Empfänger voraus. Stattdessen betrachten sie jedes Einzelteil der übertragenen Daten für sich als Ganzes, welcher mit der Adresse des letzten Empfängers ausgestattet ist und unabhängig von anderen Nachrichten zugestellt wird. Einzelne Nachrichten können auch auf andere Wege übermittelt werden.

- **Zuverlässige Dienste** stellen Services zur Verfügung, welche niemals irgendwelche Daten verlieren. Dazu gehören in der Regel Dienste, welche von einem effektiven Mechanismus für Bestätigungsmeldungen aufrechterhalten werden.

- **Unzuverlässige Dienste** stellen keine Bestätigungsmeldungen zur Verfügung, bieten jedoch Services mit hoher Zuverlässigkeit.

4.3. ISO/OSI Referenzmodell

Dieses beliebte Modell wurde von der ISO als einheitlicher Standard für miteinander verbundene Systeme verschiedener Arten und Konzepte entworfen, welche von verschiedenen Herstellern definiert wurden. Das erstellte Modell enthält sieben Schichten. Diese sieben Schichten schaffen eine komplexe Hierarchie, welche mit Anwendungen an der Spitze beginnen und mit physikalischen Verbindungen auf der untersten Ebene enden. Das OSI Referenzmodell enthält zwei Modelle der Kommunikation:

- Horizontal: protokollbasiertes Modell, über welches Programme und Prozesse verschiedener Computer kommunizieren,
- Vertikal: servicebasiertes Modell, über welches die Schichten eines einzelnen Computers miteinander kommunizieren.

Tatsächlich erfordert eine effektive Kommunikation folgende Elemente: Man benötigt zwei Seiten, welche miteinander kommunizieren möchten sowie eine gemeinsame Sprache (Protokoll), mit deren Hilfe die Seiten miteinander kommunizieren können. Darüber hinaus kommunizieren die vertikalen Schichten via API (Application Program Interface).

Anwendungsschicht
Darstellungsschicht
Sitzungsschicht
Transportschicht
Netzwerkschicht
Sicherungsschicht
Bitübertragungsschicht

4.3.1. Anwendungsschicht

Diese Schicht legt genau fest, in welcher Umgebung Netzwerkanwendungen mit dem Netzwerkdienst kommunizieren. Der Endbenutzer verwendet das Netzwerk, um die Anwendung auszuführen, Daten zu übertragen, Nachrichten zu senden, sich aus der Ferne einzuloggen usw. Die Anwendungsschicht-protokolle enthalten vor allem Anwendungsprogramme, aber auch Netzwerküberbauten, welche es der Station ermöglichen, sich mit dem Netzwerk zu verbinden. Programme und Protokolle, welche Dienste der Anwendungsschicht bereitstellen, sind mitunter:

- NICE (Network Information and Control Exchange), welches die Überwachung und Administration des Netzwerks sicherstellt.
- FTAM (File Transfer Access and Management), welches für die Dateienverwaltung aus der Ferne zuständig ist.
- X.400, welches Protokolle und Funktionen zum Versenden von Nachrichten und elektronischer Post festlegt.
- CMIP, welches für die Netzwerkadministration verantwortlich ist, die auf den von OSI definierten Rahmenbedingungen basiert.
- Telnet, welches eine Terminalemulation und Fernverbindung bereitstellt.
- Rlogin, welches eine UNIX-Umgebung mit Fernverbindung bereitstellt.

4.3.2. Darstellungsschicht

Diese Schicht gibt der Datenübertragung ihre Form. Die Daten, welche über das Netzwerk übermittelt werden, können entweder Texte, Ziffern oder allgemeine Datenstrukturen sein. Darüber hinaus enthält diese Schicht Spezifikationen für das Kodieren und Dekodieren von Zeichensätzen. Eine Datenkomprimierung und Chiffrierung kann auch in dieser Schicht stattfinden. Darüber hinaus stellt die Darstellungsschicht der direkt darüber befindlichen Anwendungsschicht Services zur Verfügung und nutzt eine Sitzungsschicht, die sich unmittelbar darunter befindet.

4.3.3. Sitzungsschicht

Auf dieser Ebene werden Prozesse angestoßen, welche den Datentransfer steuern, deckt Übermittlungs- und Übertragungsfehler fest und legt Aufzeichnungen über Rundfunkübertragungen an. Darüber hinaus unterbricht diese Schicht Sitzungen zwischen den beiden Endteilnehmern (dem Nutzer und dem Zielcomputer) bzw. hält diese aufrecht. Um eine Sitzung zu starten, bedarf es einer über die Transportschicht hergestellten Verbindung, mittels welcher eine Kommunikation zwischen den beiden Sitzungsteilnehmern ermöglicht wird. Ebenso entscheidet sie, wer Signale übermitteln kann oder unterbricht die bestehende Sitzung. Zu den Sitzungsschichtprotokollen gehören:

- ADSP (AppleTalk Data Stream Protocol): Dieses erlaubt zwei Netzwerkknoten, eine prekäre Verbindung für den Datentransfer herzustellen.
- NetBEUI bezieht sich auf die Umsetzung und Entwicklung von NetBIOS.
- NetBIOS verwendet die 5., 6. und 7. Schicht und bietet Dienste zur Sitzungsüberwachung.
- PAP (Printer Access Protocol) ermöglicht den Zugriff auf PostScript-Drucker im AppleTalk-Netzwerk.

4.3.4. Transportschicht

Diese Schicht ermöglicht die Funktionstüchtigkeit eines geeigneten Verbindungsaufbaus und splittet Daten in kleinere Teile, sprich Pakete auf, zu welchen die übertragenen Daten gebündelt werden. Nach deren Empfang werden die Daten aus dem Paket entnommen und in ihre ursprüngliche Form gebracht. Dadurch stellt diese Schicht sicher, dass beliebig große Nachrichten übertragen werden, obwohl ihre einzelnen Pakete eine begrenzte Größe haben. In der Tat ist die Transportschicht essentiell, da sie sich zwischen oberen und unteren Schichten befinden, welche netzwerkorientiert sind.

4.3.5. Netzwerkschicht

Diese Schicht beschreibt Prozesse, welche Daten zwischen Netzwerkadressen versenden und überprüfen, ob die gesamten Nachrichten rechtzeitig gesendet wurden. Darüber hinaus stellt sie einangenehmes Versenden von Paketen sicher. Die Netzwerkschicht muss überdies die besondere Netzwerktopologie kennen, sprich den Weg der direkten Verbindung der einzelnen Netzwerkknoten untereinander.

4.3.6. Sicherungsschicht

In dieser Schicht, welche auch Verbindungsschicht genannt wird, finden jene Verfahren statt, welche zum Aufspüren und Korrigieren von Fehlern auf der Datenebene während der Übertragung von Daten zwischen der Bitübertragungsschicht und den darüber liegenden Schichten dienen. Die Sicherungsschicht erstellt Pakete relevanter Netzwerkarchitektur. Trotzdem kommt es auf dem Übertragungsweg immer wieder zu Fehlern, welche zur Folge haben, dass die erhaltenen Bites sich von den versendeten unterscheiden. Die Bitübertragungsschicht kümmert sich nicht um die Relevanz einzelner Bits. Diese Art von Fehlern wird in der Sicherungsschicht aufgespürt. Diese überprüft, ob die ganzen Pakete (Verschicken unterschiedlicher Prüfsummen usw.) korrekt übertragen wurden. Darüber hinaus übermittelt die Sicherungsschicht dem Sender unmittelbar eine Empfangsbestätigung der einwandfrei übertragenen Pakete, wohingegen ein Fehler deren wiederholte Übermittlung erfordert.

4.3.7. Bitübertragungsschicht

Diese Schicht erhebt die elektrischen, mechanischen und funktionalen Anforderungen, welche an die Verarbeitung von Netzwerkdaten gestellt werden. Im Großen und Ganzen scheint die Aufgabe einfach zu sein: Die Schicht stellt die Übertragung einzelner Bits zwischen einem Empfänger und einem Sender sicher.

4.4. TCP/IP Modell

TCP/IP steht für Transmission Control Protocol/Internet Protocol. Es bezieht sich auf eine Standard-Protokolldatei, welche zB im Internetnetzwerk verwendet wird, welches zum größten Netzwerk der Welt geworden ist.

Wie die Geschichte zeigt, hat die DARPA (Defence Advanced Project Agency) 1969 ein Forschungs- und Entwicklungsprojekt gestartet, welches darauf abzielte, ein experimentelles Netzwerk mit Datenpaketvermittlung aufzubauen. Dieses Netzwerk wurde ARPANET genannt und wurde entworfen, um Methoden zu studieren, welche eine verlässliche und anbieterunabhängige Daten-kommunikation erlauben. Alles in allem war das Experiment sehr erfolgreich und eine große Zahl von Organisationen begann damit, dessen Dienste für die Alltagskommunikation zu verwenden. Im Jahr 1975 wurde das ARPANET von einem experimentellen in ein operierendes Netzwerk umgewandelt. Das Fundament für das TCP/IP-Protokoll wurde gelegt, als das ARPANET bereits ein operierendes Netzwerk war. Dieses Protokoll wurde 1983 als Militärstandard übernommen und ungefähr von diesem Zeitpunkt an verbreitete sich der Begriff Internet über den gesamten Globus.

Vorteile von TCP/IP

- Offener Protokollstandard, welcher frei verfügbar ist und unabhängig von einer bestimmten technischen Ausstattung oder eines Betriebssystems entwickelt wurde.
- Vollkommene Unabhängigkeit von einer bestimmten physikalischen Netzwerkhardware, wodurch es möglich ist, TCP/IP innerhalb einer großen Anzahl von Netzwerken zu betreiben. So kann TCP/IP mitunter über Ethernet, Token Ring, Telefonleitungen und praktisch jedes physikalischen Übertragungsmedium laufen.
- Eine allgemeine Regelung erlaubt es jedem TCP/IP-Gerät, jedes andere Gerät im gesamten Netzwerk anzusprechen.
- Standardisierte High-Level-Protokolle, welche allgemein verfügbare Nutzerdienste anbieten.

4.5. Architektur von TCP/IP-Protokollen

Protokolle entwerfen formale Verhaltensrichtlinien innerhalb des Datenverkehrs. In homogenen Netzwerken wird dieses Regelwerk vom Systemanbieter formuliert. TCP/IP erstellt ein heterogenes Netzwerk mit offenen Protokollen, welche nicht von den Unterschieden zwischen Betriebssystemen und Architekturen abhängig sind. Sie sind für jeden verfügbar und ihre Entwicklung und Anpassungen unterliegen den Vertragsbedingungen. Die genaueste Information über TCP/IP findet sich im RFC (Request for Comments): Diese Dokumente enthalten die letzten Aktualisierungen aller Standard-spezifikationen.

TCP/IP wird gemeinhin al sein Modell betrachtet, welches aus weniger Schichten als das OSI-Modell besteht. Die meisten der TCP/IP-Beschreibungen definierten die Protokollarchitektur mit drei bis fünf Ebenen.

Netzwerkschnittstellenschicht

Diese Schicht kümmert sich um alles, was man mit der Steuerung eines bestimmten Übermittlungs-pfades, der direkten Übertragung und dem Empfang von Datenpaketen verbindet. Darüber hinaus bedarf sie einer bestimmten Übermittlungstechnologie (sprich alle Industriestandards wie Ethernet, IEEE 802.x und FDDI).

Internetschicht

Diese Schicht wird manchmal auch IP-Schicht genannt, in Anlehnung an das IP-Protokoll. Sie stellt sicher, dass einzelne Pakete vom Sender zu ihrem tatsächlichen Empfänger geschickt werden – unabhängig davon, ob zwischen ihnen eine direkte Verbindung besteht. Unter Berücksichtigung des nicht-verbundenen Übertragungscharakters (IP-Protokoll) wird ein elementarer Datagrammdienst auf der Ebene dieser Schicht bereitgestellt.

Das Internetprotokoll ist ein Eckpfeiler des Internets. Zu seinen Funktionen gehören:

- die Datagrammdefinition, welche die grundlegende Übermittlungseinheit ist,
- die Definition des Internetadressschemas,
- die Datenübertragung zwischen der Netzwerk- und Transportschicht,
- das Hinführen von Datagrammen zu entfernten Zielen,
- das Bereitstellen einer Fragmentierung und eines Datagrammaufbaus.

Datagramm bezieht sich auf ein Paketformat (Paket ist ein Datenblock, welcher Informationen enthält, die für dessen Zustellung notwendig sind), welches vom Internetprotokoll definiert ist.

Transportschicht

Diese Schicht wird gemäß des Protokolls auch TCP-Schicht genannt. Sie ist dafür zustän-

Übermittlung zwischen den Endteilnehmern sicherzustellen, welche im Fall einer TCP/IP-Architektur Anwendungsprogramme sind. Je nach deren Anforderungen kann die Transportschicht den Daten-fluss in beide Richtungen regulieren, die Übermittlungszuverlässigkeit sicherstellen und auch den nicht-verbundenen Charakter der Übertragung innerhalb der Netzwerkschicht in einen verbundenen Charakter ändern.

Anwendungsschicht

Die Anwendungsschicht ist die oberste Schicht der TCP/IP-Architektur: Ihre Entitäten repräsentieren individuelle Anwendungsprogramme, welche – im Gegensatz zu RM OSI – direct mit der Transport-schicht kommunizieren. Mögliche Darstellungs- und relationale Dienste werden von den Anwendungsprogrammen selbst bereitgestellt.

4.6. Architektur kommunizierender Systeme

Begriffsbestimmungen

- **System**
  - ein unabhängiges Ganzes, welches in der Lage ist, Prozesse und Übertragungsinformationen anzuregen

- **Netzwerkarchitektur**
  - System aus Schichten, Diensten, Funktionen und Protokollen
  - stimmt mit der Struktur der Netzwerkausstattung überein

- **Offene Architektur**
  - entsprechende Standards, welche die Architektur beschreiben, sind öffentlich zugänglich
  - alle Systeme, welche die Standards erfüllen, sind miteinander verknüpfbar

- **Schichtprotokoll**
  - Kooperationsregeln der Entitäten derselben Schicht und anderer Systeme

- **Schnittstellenprotokoll**
  - SW-Schnittstelle
  - Kooperationsregeln von benachbarten Schichten
  - Dienstelemente werden verwendet
  - Kommunikation über Service Access Points (SAP)

5. ISO/OSI MODELL, AUSGEWÄHLTEN PROTOKOLLE

5.1. Computernetzwerke - ISO/OSI-Modell

Das ISO/OSI-Modell bezeichnet ein Kommunikationsmodell, welches “International Standards Organization/Open System Interconnection“ genannt wird. Es bezieht sich auf ein empfohlenes Modell, welches von der ISO im Jahr 1983 definiert wurde. Dieses teilt die übliche Kommunikation zwischen Computern in sieben miteinander verbundene Schichten auf. Die entsprechenden Schichten werden als Protokollschichtensatz bezeichnet.

Die Hauptaufgabe jeder Schicht ist es, der jeweils darüber befindlichen Schicht bestimmte Services bereitzustellen und eben jene übergeordnete Schicht nicht mit Details über die bestimmte Service-bereitstellung zu belasten. Bevor Daten von einer Schicht in die andere übertragen werden, werden diese in Pakete unterteilt. In der Folge werden alle Pakete in jeder Schicht mit zusätzlichen Informationen (Format, Adresse) angereichert, welche für eine erfolgreiche Übertragung über das Netzwerk notwendig sind.

Das vorgeschlagene Modell zeigt die folgenden Schichten (jede übergeordnete Schicht nutzt Funktionen der darunter befindlichen Schicht).

Eine kurze Beschreibung der einzelnen Schichten: Die einzelnen Schichten werden in derselben Reihenfolge erklärt, wie sie in der Grafik nummeriert sind.

1. Bitübertragungsschicht

Diese definiert Kommunikationsmittel mit einem mobile Medium und die technischen Mittel der Schnittstelle. Darüber hinaus definiert sie die physikalischen, elektrischen, mechanischen und funktionellen Parameter, welche sich auf die physische Verbindung der einzelnen Komponenten beziehen. Das heißt, sie befasst sich mit der Hardware.

2. Sicherungsschicht

Diese hält die Integrität des Datenflusses von einem Netzwerkknoten zu einem anderen aufrecht. Diese Aktivität umfasst auch die Datenblocksynchronisierung und deren Flussteuerung. Diese Schicht befasst sich folglich auch mit der Hardware.

3. Netzwerkschicht

Diese legt Protokolle für Datenrichtungen fest, über welche der Informationstransfer zum erforderlichen Netzwerkknoten sichergestellt wird. Dies bedeutet, dass die richtige Richtung – außer, man entscheidet sich dafür – nicht im lokalen Netzwerk sein muss. Diese Schicht bezieht sich auch auf die Hardware: Wenn sich der PC jedoch mit der Richtung zwischen zwei Netzwerkkarten befasst, betrifft sie die Software.

4. Transportschicht

Diese definiert die Protokolle für strukturierte Nachrichten und stellt deren einwandfreien Transfer sicher (übernimmt ein paar Fehlerüberprüfungen). Darüber hinaus stellt sie die Partitionierung in Pakete und die Bestätigung sicher. Diese Schicht befindet sich auf der Software-Ebene.

5. Sitzungsschicht

Diese koordiniert die Kommunikation und hält Sitzungen so lange wie notwendig aufrecht. Ebenso übernimmt sie Sicherheits-, Anmeldungs- und Verwaltungsfunktionen. Sie bezieht sich auf Software.

6. Darstellungsschicht

Diese erkundet den Art und Weise der Datenformatierung, -darstellung, -umwandlung und -kodierung. Das heißt, sie beschäftigt sich mit Umlauten, Interpunktion, (De-)Komprimierung und Datenverschlüsselung. Sie befindet sich ebenfalls auf der Software-Ebene.

7. Anwendungsschicht

Hierbei handelt es sich um die oberste Schicht. Sie erkundet die Art und Weise, auf bzw. über die Netzwerke mit Anwendungen kommunizieren können, zB Datenbanksysteme, elektronische Post oder Programme für Terminalemulationen. Sie nutzt Dienste darunter befindlicher Schichten, wo-durch sie von Problemen technischer Netzwerkressourcen abgegrenzt wird. Sie ist softwarebasiert.

5.2. ISO/OSI-Referenzmodell: Sieben Schichten

Die Architekten des ISO/OSI-Referenzmodells kamen überein, dass eine Netzwerksoftware idealerweise sieben Schichten haben sollte. Es bleibt jedoch noch die Frage zu klären, mit welchen Schichten bzw. welchen damit verbundenen Aufgaben man sich auseinandersetzen muss. Auf eben diese wird nachfolgend in hierarchisch aufsteigender Reihenfolge eingegangen:

1. Bitübertragungsschicht

Ihre Hauptaufgabe scheint recht einfach zu sein: Eine Übertragung von einzelnen Bits zwischen dem Empfänger und dem Sender über einen physikalischen Transferpfad zu gewährleisten, welcher sich unter vollständiger Kontrolle dieser Schicht befindet. Nichtsdestotrotz muss man sich mit einer Reihe von Problemen technischer Natur beschäftigen, zB dem Spannungsniveau der Logik 1 und der Logik 0, wie lange ein Bit „währt", wie viele Kontakte und welche Form Kabelanschlüsse haben sollten, welche Signale über diese Kabel übermittelt werden, welche Relevanz diese haben, deren Zeitverlauf usw. Deshalb fallen diese Angelegenheiten eher in den Kompetenzbereich der Elektroingenieure und Techniker.

2. Sicherungsschicht

Die Bitübertragungsschicht stellt in der Regel Mittel zum individuellen Bittransfer als Standarddienste bereit. Durch die Verwendung dieser Services muss die darüber befindliche Sicherungsschicht (manchmal auch Verbindungsschicht) eine einwandfreie Übertragung von Datenblöcken (im Umfang von hunderten von Bits), welche Frames genannt werden, sicherstellen. Da die Bitübertragungs-schicht keine einzelnen Bits interpretiert, muss die Sicherungsschicht den Anfang und das Ende des Frames sowie dessen Einzelteile korrekt definieren.

In der Tat können zahlreiche Unterbrechungen und Fehler auf dem Transferpfad auftauchen, welche dazu führen, dass empfangene Bit-Werte von den gesendeten abweichen. Da die Bitübertragungs-schicht sich jedoch nicht mit einzelnen Bits beschäftigt, werden diese Fehler erst in der Sicherungs-schicht festgestellt. Diese Schicht überprüft die gesamten Frames darauf, ob sie korrekt übertragen wurden (gemäß der Prüfsumme, siehe Kapitel 3). Darüber hinaus stellt sie dem Sender Informationen über die einwandfreie Übertragung von Frames zur Verfügung, wobei sie gleichzeitig – im Falle von beschädigten Frames – deren erneutes Senden erfordert.

3. Netzwerkschicht

Die Sicherungsschicht stellt die Übertragung ganzer Frames sicher, jedoch nur zwischen zwei Netzwerkknoten, zwischen welchen eine direkte Verbindung besteht. Bleibt die Frage, was zu tun ist, wenn man davon ausgeht, dass die Verbindung zwischen einem

Empfänger und einem Sender nicht direkt, sondern über einen oder mehrere zwischengeschaltete Knoten läuft? Hier kommt die Netzwerkschicht ins Spiel, welche ein komfortables Routing der übertragenen Frames, welche als Pakete bezeichnet werden, sicherstellt. Die Netzwerkschicht wählt den korrekten Pfad (oder die korrekte Route) über zwischengeschaltete Knoten aus und stellt darüber hinaus den progressiven Transfer einzelner Pakete auf der Route vom ursprünglichen Sender hin zum finalen Empfänger sicher. Deshalb muss die Netzwerkschicht eine bestimmte Netzwerktopologie beachten (sprich den Weg der direkten Verbindung einzelner Knoten).

4. Transportschicht

Die Netzwerkschicht stellt der darüber liegenden Schicht Dienste bereit, welche den Pakettransfer zwischen zwei willkürlich gewählten Netzwerkknoten sicherstellt. Daraus folgt, dass die Transport- schichtaus der tatsächlichen Netzwerktopologie herausgefiltert wird und die Illusion erzeugt, dass jeder Netzwerkknoten eine direkte Verbindung zu jedem beliebigen anderen Netzwerkknoten hat. Folglich stellt die Transportschicht nur eine Ende-zu-Ende-Kommunikation sicher, sprich die Kommunikation zwischen dem ursprünglichen Sender und dem finalen Empfänger.

Darüber hinaus sorgt die Transportschicht dafür, dass im Zuge der Datenübertragung einzelne Pakete gebildet werden, in welche die übertragenen Daten unterteilt werden. Auf dieselbe Weise werden die Daten nach ihrem Erhalt aus den Paketen entnommen und wieder in ihre ursprüngliche Form gebracht. Dadurch wird die Übertragung eines Inhalts beliebiger Größe sichergestellt, obwohl die einzelnen Pakete eine begrenzte Größe haben.

5. Sitzungsschicht

Diese Schicht stellt Sitzungen zwischen Endteilnehmern her, hält diese aufrecht und unterbricht sie. Während des Sitzungsaufbaus erfordert diese Schicht eine Verbindung zur Transportschicht, über welche eine Kommunikation zwischen den beiden Sitzungsteilnehmern herstellt wird. Diese Schicht ist für ein fallweises Kommunikationsmanagement zuständig (sprich den Entwurf des Übermittlungs-zeitplans beim gleichzeitigen Auftauchen zweier Teilnehmer). Darüber hinaus ist die Schicht für alles zuständig, was mit dem Abbruch der Sitzung und der bestehenden Verbindung zusammenhängt

6. Darstellungsschicht

Die Daten, welche über das Netzwerk übertragen werden, können unter anderem textuell oder numerisch sein oder bloß gewöhnliche Datenstrukturen. Einzelne Knotencomputer können jedoch verschiedene interne Darstellungen dieser Daten verwenden. So nutzen zentrale Computer der Firma IBM einen EBCDIC-Zeichencode, während die meisten anderen mit einem ASCII-Code arbeiten. Ebenso kann ein Computer Integer im Zusatzcode

anzeigen, während sie bei anderen vielleicht im direkten Code aufscheinen usw. Diese Schicht ist für die erforderliche Konvertierung der übertragenen Daten zuständig.

Diese Schicht übernimmt auch potentielle Komprimierungen übertragener Daten oder alternative deren Chiffrierung.

7. Anwendungsschicht

Endnutzer greifen über verschiedene Netzwerkanwendungen auf Computernetzwerke zu: elektronische Postsysteme, Datentransfer, Fernanmeldung usw. Klarerweise braucht man angesichts ihrer enormen Vielfalt nicht einmal an das direkte Einbauen all dieser verschiedenen Anwendungen in die Anwendungsschicht zu denken. Aus diesem Grund umfasst die Anwendungsschicht nur einen Teil dieser Anwendungen, welche übliche, sprich allgemein anwendbare Mechanismen zur Verfügung stellen. Nimmt man die elektronische Post (Mail) als Beispiel, so sieht man, dass ein bestimmter Teil, welcher Netzwerkmeldungen sicherstellt, auch ein integraler Bestandteil der Anwendungsschicht ist. Bei allen Knoten-Computern, welche dasselbe elektronische Mailsystem verwenden, ist dieser Teil identisch. Die Benutzerschnittstelle des elektronischen Mailsystems, sprich eben jener Teil, welcher tatsächlich vom Benutzer verwendet wird und es diesem erlaubt, Nachrichten zu lesen, darauf zu antworten, neue zu verfassen und diese zum Versand aufgibt, wird nicht länger als ein Teil der Anwendungsschicht betrachtet, da sich dieser in jedem bestimmten Knoten deutlich unterscheiden kann, zB im Hinblick auf die Bedienung (durch Zeilenbefehle, verschiedene Menüarten, mit oder ohne Fenster usw.). Ein weiteres typisches Beispiel wäre eine Terminalemulation, welche für eine Fernanmeldung benötigt wird. Alles in allem gibt es eine große Zahl an verschiedenen Terminals, was es fast unmöglich macht, die erforderliche Anpassung zwischen zwei beliebigen Terminalarten zu erreichen. Die Konsequenz daraus ist, dass nur ein „Referenzterminal“ – ein so genanntes virtuelles Terminal – implementiert wird. Jede bestimmte Terminalart besitzt nur eine Anpassung an eben dieses virtuelle Terminal. Nichtsdestotrotz finden sich die Mittel, um mit diesem virtuellen Terminal zu arbeiten, in der Anwendungsschicht (da diese identisch sind), während sich die Mittel zur Anpassung an ein bestimmtes Terminal nicht in der Anwendungsschicht befinden.

6. DRAHTLOSE KOMMUNIKATIONS-TECHNOLOGIEN

Kabellose Netzwerke; Grundsätze, Standards, Komponenten, Kommunikations-art, Anwendung und Eigenschaften.

Standards

Die Entwicklung drahtloser Netzwerke ging ziemlich ähnlich vonstatten wie jene von Kabelnetzwerken. Erfolgte sie zu Anfang noch relative spontan, wurde es bald notwendig, Standards zu definieren, welche eine allgemeine Netzwerkkooperation ermöglichten. Die wichtigsten Hersteller drahtloser Technologie schlossen sich zur WECA zusammen (Wireless Ethernet Compatibility Alliance), die Vorgaben betreffend dessen effektives Management machte und auf diesem Weg eine allgemeine Kompatibilität sicherstellte. Erfüllt ein Produkt diese festgelegten Voraussetzungen, erhält es ein WiFi-Zertifikat, welches bescheinigt, dass es mit Produkten anderer Hersteller kompatibel ist. Der kabellose Standard selbst basiert auf dem Ethernet, weshalb sie ähnliche Merkmale haben, sprich eine CSMA/CD Zugriffsmethode und einen ähnlichen Paketaufbau. Es gibt zahlreiche Standards für drahtlose LAN-Netzwerke, dessen Eigenschaften in der Tabelle skizziert werden. Der 801.11g-Standard ist rückwärts-kompatibel mit dem älteren und langsameren 802.11b (sie können miteinander arbeiten, allerdings nur mit geringerer Geschwindigkeit). Der 802.11i-Standard basiert auf dem 802.11g-Standard, wobei der ältere von beiden einen sichereren Authentifizierungs- und Chiffrierungsalgorithmus nutzt.

Komponenten

Drahtlose Komponenten kommunizieren auf zwei nützliche Arten:

- **Ad hoc**, was sich auf eine direkte Verbindung zwischen mehreren Computern bezieht, sprich zwei bis fünf. Jeder Computer kommuniziert mit einem anderen auf derselben Ebene, sprich sie sind gleichwertig (die Organisation ist einem Peer-to-Peer-Netzwerk ähnlich). Die größten Vorteile sind die schnelle Installation und der geringe Preis (bis auf Client-Netzwerkadapter benötigt man keine andere Hardware). Es ermöglicht das Teilen von Dateien und des Internetzugangs, das Drucken über das Netzwerk und andere Dinge, welche gemeinhin in LANs auftauchen. Auf der anderen Seite ist ein wesentlicher Nachteil, dass alle verbundenen Geräte in einer bestimmten Reichweite sein müssen, sprich jedes Gerät muss das andere sehen. Eine weitere Schwachstelle ist die lächerlich einfach herzustellende Verbindung, welche man nicht als besonders sicher betrachten kann.

- Der Infrastrukturmodus basiert auf einem **Access Point (AP)**. Dieser fungiert als Server, über welchen der gesamte Datenfluss zwischen Netzwerk-Clients stattfindet (die Organisation ist ähnlich zum Client-/Server-Netzwerk). Der größte Vorteil

seines Einsatzes ist die Möglichkeit, die Operation zu filter und zu überwachen sowie das Bereitstellen von Netzwerken für verschiedene Clients. Somit wird sichergestellt, dass unbewusste Versuche, eine Ad-hoc-Verbindung herzustellen, unterbunden werden. Der gesamte Datenfluss muss zum AP geleitet werden, welcher einen adäquaten Netzwerkschutz gewährleistet. Der Zugangspunkt ist definitiv nicht notwendig, wenn man davon ausgeht, dass eine drahtlose Verbindung nur gelegentlich und nur zwischen ein paar Geräten hergestellt wird. Wird jedoch ein Heimnetzwerk aufgebaut oder in einem Haushalt bzw. einem kleinen Büro geteilt, wird ein Zugangs-punkt in der Regel benötigt (höhere Netzwerksicherheit).

Access Point

Ein AP (Zugangspunkt) ist die Grundlage für ein drahtloses Netzwerk. Er stellt eine Verbindung zwischen drahtlosen Endpunkten und einem Server her, indem er ihn innerhalb eines metallischen LAN-Netzwerks platziert. Deshalb enthält ein AP eine Funkkomponente – Transmitter/Receiver und einen Kabelteil, sprich eine RJ-45-Buchse für einen Twisted-Pair-Anschluss. Zu einem AP gehören Hubs, welche das Signal übertragen. Viele Hersteller bieten den Betrieb des APs mittels Twisted-Pair-Kabel an, über welches der Zugangspunkt mit einem festen Netzwerk verbunden ist. Daher muss der Zugangspunkt (an einer schwer zugänglichen Stelle) nicht die Last zweier Kabelleitungen tragen. Der Zugangspunkt und seine Gegenstücke – Client-Adapter funktionieren, solange es kein Hindernis gibt – zwischen dem Zugangspunkt und den Computern, welche sich im drahtlosen Netzwerk befinden, müssen deutlich sichtbar sein. Eine Folge davon ist, dass man Zugangspunkte vor allem in den obersten Teilen von Räumen finden kann. Bei ihrer Positionierung muss man auf die Ursachen von Funksignalinterferenzen achten, sprich Metallkonstruktionen (auch in Wänden), elektronische Interferenzen (zB funktionieren Mikrowellen in einem Intervall von 2.4 GHz, Mobiltelefone, drahtlose Lautsprecher usw.). Solange eine direkte drahtlose Verbindung benötigt wird, lässt sich eine Wireless Bridge (WB) einsetzen – Zugangspunkte einer Brückenfunktion – welche Pakete zwischen Netzwerken herausfiltert.

Client-Adapter

Dieser Begriff bezeichnet jene Einheit, über welche ein PC mit einem Zugangspunkt verbunden ist. Im Grunde bezieht er sich auf die Netzwerkkarte (mit einer Antenne). Entwickelt wurde er für PCI- und USB-Anschlüsse. Laptops können eine Netzwerkkarte gemäß eines PC-Karten-Standards einsetzen. Allerdings besitzen die meisten Laptops bereits eine integrierte Drahtlosnetzwerkschnittstelle (welche das Aufsetzen und Abgrenzen eines drahtlosen Netzwerks erleichtert).

6.1. Eigenschaften drahtloser Netzwerke

6.1.1. Geschwindigkeit

Im Gegensatz zu metallischen Netzwerken ist deren Geschwindigkeit erheblich geringer. Die theoretisch maximal erreichbare Geschwindigkeit ist in der Tabelle vermerkt, in welchen auch adäquate Standards bereitgestellt werden. Tatsächlich sind diese Standards schwer zu erreichen, ein Umstand, welcher der schwächeren Erreichbarkeit des Signals zwischen den Funkstationen geschuldet ist, was wiederum dazu führt, das automatisch auf eine geringere Übermittlungsgeschwindigkeit umgestellt wird.

Alles in allem bedeutet das, dass seine längere Strecke (zB mehr als 20 Meter) oder ein Hindernis (zB ein dicker Metallrahmen) die Verbindungsgeschwindigkeit dramatisch reduzieren – um ein Drittel oder um die Hälfte. Solange die Gruppe von Empfängern mit demselben Zugangspunkt verbunden ist, womit sie sich physisch in einem Netzwerksegment befinden, muss die Kapazität von einem Adapter aufgeteilt werden. In der Folge treten viele Kollisionen auf (CSMA/CD Charakter). Eine weitere Variable, welche die realisierbare Geschwindigkeit verringert, ist die sorgfältige Protokollverwaltung in den oberen Schichten, bedingt durch welche sich die tatsächliche Bandbreite für den Transfer reiner Daten merklich reduziert. Gleichwohl beträgt die maximale Bandbreite für die Nutzdatenbelastung unter idealen Bedingungen ungefähr die Hälfte der Nominalwerte, sprich 5 Mbit/s bei einer B-Leitung und 25 Mbit/s bei einer G-Leitung.

6.1.2. Sicherheit

SSID (Service Set ID)

Dieser Begriff bezieht sich auf einen Zugangspunkt, welcher für alle Clients sichtbar ist, welche sich innerhalb seiner Reichweite befinden. Aus diesem Grund dient SSID als logischer Indikator für ein bestimmtes drahtloses Netzwerk. Eine SSID kann manuell an der Station angebracht werden. Alternativ kann der Zugangspunkt regelmäßig Informationen über SSID übermitteln oder die SSID-Übermittlung kann in der Situation unterbrochen werden, in welcher der Client selbst nach der SSID fragt.

WEP (Wired Equivalent Privacy)

Dieser Begriff bezeichnet ein altes Sicherheitssystem drahtloser Netzwerke nach dem ursprünglichen IEEE 802.11-Standard. Der Zweck des WEP war es, größtmögliche Sicherheit für verkabelte Computernetzwerke zu gewährleisten (zB Twisted Pair), da das Funksignal leicht selbst über eine längere Distanz hinweg ohne physischen Kontakt mit einem Computernetzwerk aufgefangen werden kann. WEP wurde im August 2001 jedoch geknackt,

weshalb es durch das dem IEEE 802.11i-Standard entsprechenden WPA2 ersetzt werden sollte.

WPA (Wi-Fi Protected Access)

Dieser Begriff bezeichnet ein Sicherheitssystem drahtloser Netzwerke. Um das Sicherheits-system WEP im Jahr 2001 zu ersetzen, verbesserte die Wi-Fi Alliance das Sicherheitssystem WPA als Teil des damals im Jahr 2002 vorbereiteten Standards IEEE 802.11i. Überdies hält die Wi-Fi Alliance die Rechte an den Marken Wi-Fi und WPA und zertifiziert ihre Produkte.

WPA2

Es implementiert alle notwendigen Komponenten des IEEE 802.11i. Es nutzt die Blockverschlüsselung des Advanced Encryption Standard (AES), wohingegen die früheren WEP und WPA die aktuelle RC4-Chiffrierung verwenden. Die Architektur von 802.11i enthält die folgenden Komponenten: IEEE 802.1X für die Bestätigung (sprich Extensible Authentication Protokoll – EAP).

Wireless PAN

WPAN verbindet einzelne Geräte in einem relativ kleinen Gebiet miteinander, auf welches eine Person, welche mit dem Netzwerk verbunden ist, leicht zugreifen kann. So können Kopfhörer zB via Bluetooth oder Infrarot mit einem Laptop verbunden sein. Auf diese Weise wird ein kleines privates Drahtlosnetzwerk erzeugt (WPAN). Zig Bee unterstützt auch WPAN-Anwendungen. In der Tat haben sich private Wi-Fi-Netzwerke aufgrund der integrierten Ausstattung einer großen Bandbreite von elektronischen Geräten zu einem Gemeingut für den typischen Konsumenten entwickelt. Darüber hinaus erleichtern Geräte wie “My Wi-Fi” von Intel und “Virtual Wi-Fi” von Windows 7 das Aufsetzen und Konfigurieren eines privaten Drahtlosnetzwerks.

Wireless WWAN

Der Begriff WWAN bezieht sich auf ein drahtloses Netzwerk, welches große Gebiete abdeckt. Diese Netzwerke können zum Verbinden von Geschäftsstellen oder als öffentliches Zugangssystem verwendet werden. Eine drahtlose Verbindung kommt in der Regel durch eine Punkt-zu-Punkt-Mikrowellenleitung zustande, welche einen Parabolspiegels mit einer Frequenz von 2.4 GHz verwendet. Ein typisches System läuft auf den Eingängen zu Basis-stationen, Zugangspunkten und drahtlosen Signalbrücken. Die andere Konfiguration umfasst Netzwerksysteme, in welchen jeder Zugangspunkt das Signal weitergibt.

Wireless MAN

Wireless Metropolitan Networks WMAN bezeichnen drahtlose Netzwerke, welch emit mehreren lokalen Netzwerken verbunden sind. WiMAX ist eine Art drahtloses MAN Netzwerk und wird durch den IEEE 802.16-Standard definiert.

6.1.3. Anwendung

Angewendet werden sie vor allem von Mobiltelefonen, welche ein integraler Bestandteil der täglichen Drahtloskommunikation sind und die Kommunikation erleichtern, die über inter-kontinentale Netzwerksysteme erfolgt, welche auf der ganzen Welt Kommunikations-satelliten einsetzen. Gemeinhin nutzen Privatpersonen und Geschäftsleute drahtlose Netzwerke zum schnellen Versenden und Teilen von Daten, unabhängig davon, ob sie sich in einem kleinen Büro oder irgendwo anders auf der Welt befinden.

7. VIRTUELLE NETZWERKE (VLAN).

VLAN ist die Abkürzung für Virtual Local Area Network. Der Begriff bezeichnet ein funktionales LAN, in welchem ein anderes, ein virtuelles Netzwerk, gebildet wird. Es läuft nur auf einem Hardware-Gerät (physische Verkabelung). Kurz gesagt operiert ein VLAN auf der Grundlage der individuellen Voreinstellung bereits aktiver Netzwerkkomponenten eines neuen virtuellen Modus und Modells.

Ein VLAN arbeitet nach Grundsatz des Taggens von Daten, welche über das Netzwerk übertragen werden. Diese Daten werden gemäß des entsprechenden virtuellen Netzwerks getaggt. Das Hauptziel ist es, mehrere lokale LANs ordnungsgemäß auf der Ebene der zweiten Netzwerkschicht des ISO/OSI-Modells miteinander zu verbinden. Darüber hinaus ist ein großer Vorteil von VLANs deren gute Konfigurierbarkeit.

Unter dem Gesichtspunkt einer qualitativ hochwertigen Netzwerksicherheit lässt sich sagen, dass ein VLAN leicht zwischen Nutzern einzelner Ende-zu-Ende-Stationen und permanent laufenden Anwendungen (z.B. Linux Demon) unterscheiden kann, unabhängig vom aktiven Netzwerkgerät.

Dadurch ist der unautorisierte Zugriff eines unethisch handelnden Hackers auf ein Computernetzwerk völlig ausgeschlossen. Die gängigste Art eines Cyber-Angriffs zielt somit auf die Computernetzwerke selbst ab, wobei einer DDoS-Attacke zu Anfang widerstanden werden kann.

7.1. Wozu braucht man ein VLAN?

Zum ersten Mal veröffentlicht wurde die VLAN-Technologie Mitte der 1990er. Einer von vielen Gründen in diesem Zusammenhang war die Bildung einer Gruppe von bestimmten Nutzern, welche auf einem einfacheren Weg erfolgreich miteinander kommunizieren und auf ihre Daten und Informationen zugreifen können sollten. Ein weiterer Grund war die Stagnierung bei der Entwicklung der Ethernet-Technologie.

Von Relevanz ist auch die Tatsache, dass die VLAN-Technologie problemlos eine Netzwerkkommunikation erkennt, welche vor kurzem ein Netzwerk auf einem geeigneten Netzwerkgerät geteilt hat – Verteiler. In der Tat stellt die Nutzung eines Verteiler-Anschlusses die effektivste und praktikabelste Lösung dar.

Die VLAN-Technologie wurde 1995 entwickelt. Sie basierte jedoch nur auf einer Close-Source-Technologie. Bis vor ein paar Jahren jedoch wurde es hauptsächlich für mittlere und Großunternehmen entwickelt, obwohl bereits ein geeigneter Standard definiert wurde.

Hauptgründe für den Aufbau eines VLANs:

- Einteilen von Netzwerknutzern in Gruppen, Bereiche oder nach bestimmten Diensten anstatt nach einer physikalischen Position und Kommunikationsabschnitten zwischen diesen Gruppen.

- Verringerung von Netzwerkübertragungen, welche vor Jahren zum Problem wurden
- Rechtzeitiges Reduzieren der Collision Domain, welche auftritt, wenn Netzknoten anstelle von Netzwerkweichen verwendet werden.

Die Idee von einer logischen Gruppe von Nutzern wird in der Literatur des Öfteren erwähnt. Ihr zufolge wird bei der Bildung eines VLANs Folgendes beachtet:

- **Organisationelle Struktur:** Die Voraussetzung, dass die Kommunikation innerhalb des Bereichs mit Druckern, Datenservern usw. realisiert wird. Die Voraussetzung, dass es keine Kommunikation zwischen einzelnen Abschnitten gibt. Nur ein paar Dienste (zB Mail) sind üblich.

- **Dienste:** VLAN vernetzt Mitarbeiter, welche dieselben Dienste nutzen (zB Buchhaltung, DB usw.)

Die größen Vorteile von VLAN

Da sich die VLAN-Zugehörigkeit auf verschiedene Arten definieren lässt, werden VLANs typischerweise in Netzwerke mit Port-basierter und regelbasierter Zugehörigkeit unterteilt. Eine etwas differenziertere Unterteilung kennt vier Arten von VLAN-Zugehörigkeit:

- Ports,
- MAC-Adressen von Netzknoten,
- Netzwerkprotokoll oder Netzwerkadressen von Netzknoten,
- Gruppe der IP-Übertragung

Port-basiertes VLAN

Diese historisch gesehen erste virtuelle Netzwerkart legt die Netzwerkzugehörigkeit einzelner Verteiler-Ports (Portgruppen) fest. Die ersten VLAN-Umsetzungen erlaubten keine Erweiterung des virtuellen Netzwerks um mehrere Verteiler. Sie konzentrierten sich auf eine Netzwerkweiche. Auch die darauffolgende Generation erlaubte dies noch nicht. Nachfolgend ist ein solches definiertes Netzwerk abgebildet.

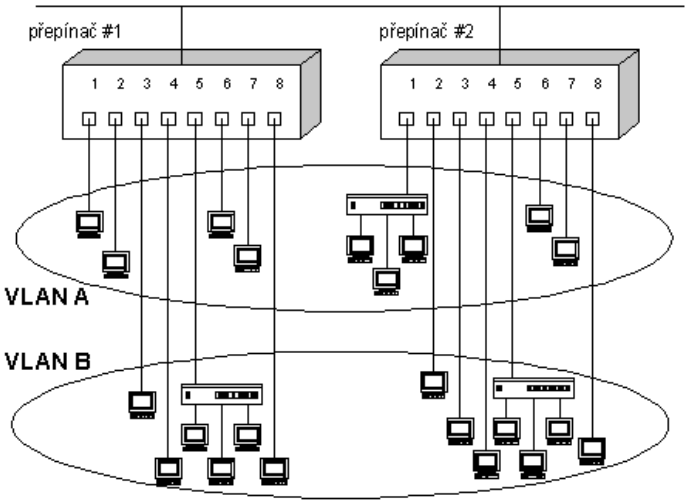


Abb.: Port-basierte VLAN-Zugehörigkeit

Das Gruppieren von Ports ist das Standardprinzip bei der Erstellung eines virtuellen Netzwerks. Obwohl es sehr klar und einfach ist, besteht seine Haupteinschränkung darin, die Zugehörigkeit im Zusammenhang mit jeglicher Verschiebung der Nutzerstation zwischen einzelnen Verteilerports neu definieren zu müssen (sprich solche Veränderungen hätten eine Veränderung der Zugehörigkeit im virtuellen Netzwerk zur Folge).

MAC-Adressen basiertes VLAN

Eine MAC-Adresse ist im Netzwerkadapter-Kreislauf „in Bedrängnis". Deshalb kann man auf diese Weise definierte virtuelle Netzwerke als nutzerbasierte VLANs betrachten. Geht man davon aus, dass sein Nutzer seine Verbindung ändert (sprich seine Station an einen anderen Verteilerport verlagert), bleibt seine VLAN-Zugehörigkeit dennoch dieselbe.

Diese Methode erfordert eine starre, manuelle Zuweisung der Zugehörigkeit aller Netzwerke einer Station. Ein weiterer großer Nachteil ist die Gefahr einer substanziellen Leistungs-verringerung im Falle eines geteilten Segments, in welchem Stationen verschiedener VLANs mit dem Verteilerport verbunden sind. Das nächste, wenn auch eher kleine, Problem kann auftreten, wenn Nutzer und ihre Laptops ihren Standort ändern und sich über eine permanent angeschlossene Docking-Station mit dem Netzwerk verbinden. Dadurch ändert sich mit dem Standort auch die festgelegte MAC-Adresse (der Netzwerk-Adapter ist im Wesentlichen ein Teil des Docks). Obwohl dies nur ein kleines Problem darstellt, treten bestimmte VLAN-Grenzen zutage, die sich durch eine MAC-Adressen basierte Zugehörigkeit ergeben.

Darüber hinaus sorgt die Möglichkeit der Nutzer, ihre eigene MAC-Adresse direkt im Betriebssystem umzustellen, für weitere Schwierigkeiten, vor allem in Hinblick auf die Sicherheit.

Protokoll- oder adressenbasiertes VLAN

Solche virtuellen Netzwerke basieren auf den Informationen der dritten Netzwerkschicht des OSI-Modells. In Netzwerken mit mehreren Protokollen können Netzknoten nach ihren operierenden Netzwerkprotokollen in einzelne VLANs eingeteilt werden, oder zB in Netzwerke mit TCP/IP-Protokoll entsprechend der Subnetzwerk-Adresse.

Obwohl es hier um Informationen über die Netzwerkschicht geht, ist es wichtig festzuhalten, wir uns nicht mit deren Nutzung für das Routing beschäftigen. Obwohl der Verteiler das Paket überprüfen muss, um die IP-Adresse und damit auch die VLAN-Zugehörigkeit zu spezifizieren, werden keine Routing-Berechnungen durchgeführt. Der Verteiler nutzt keine Routing-Protokolle (wie RIP, OSPF). Folglich muss das VLAN, welches entsprechend den Informationen der dritten Netzwerkschicht definiert wurde, als Netzwerk mit einer flachen Topologie betrachtet werden, das mittels Verteilern oder Brücken zusammengeschaltet ist.

Das gleichmäßige Verteilen in der dritten Netzwerkschicht und der Einsatz von Verteilern mit eingebauter Routingfähigkeit verringern auf den ersten Blick das Problem. Dieses betrifft jedoch verschiedene Funktionen: Einerseits das bloße Ermitteln der VLAN-Zugehörigkeit basierend auf der Netzwerkadresse, andererseits die vollständige Nutzung der Router-fähigkeiten auf Grundlage der Routingprotokolle und Berechnungen. Es ist auch wichtig zu sagen, dass die Kommunikation zwischen einzelnen VLANs den Einsatz von Routern erfordert – egal, ob es sich um klassische Router oder Verteiler mit eingebauten Routing-Funktionen handelt. Gleichzeitig hat das Definieren eines Netzwerkschicht-basierten VLANs eine Reihe von Vorteilen, zB die Nutzermobilität. Genauer gesagt bezieht sich das auf ihre Stationen,

- für welche ein erneutes Konfigurieren der VLAN-Zugehörigkeit nicht notwendig ist,
- welche Gruppen bilden können, die bestimmte Dienste bereitstellen
- oder das (Ab-)Schaffen der Notwendigkeit des Pakettaggings, welches Informationen über die VLAN-Zugehörigkeit enthält, wenn sie miteinander kommunizieren (siehe nachfolgende Absätze).

Gruppenfunkbasiertes VLAN

Der Gruppenfunk in IP-Netzwerken (IP Multicast) funktioniert folgendermaßen: Ein Paket, welches für den Gruppenfunk entwickelt wurde, wird an eine bestimmte Adresse geschickt, die als Proxy für eine ausdrücklich festgelegte Gruppe von Netzwerkknoten (IP-Adressen) funktioniert. Das Paket wird an alle Netzknoten gesendet, welche zu dieser bestimmten Gruppe gehören. Diese Gruppe wird auf dynamischer Grundlage gebildet: Innerhalb dieser Gruppen loggen sich die Netzknoten ständig ein und aus. Folglich können alle Stationen als Mitglieder eines virtuellen LANs betrachtet werden, da die Gruppe eine Domain des Rundstrahlbetriebs bilden. Trotzdem unterscheidet sich das Gruppenfunk-

basierte VLAN in zwei markanten Punkten: Die Gruppe wird nur temporär dynamisch gebildet. Daher ist das Netzwerk sehr flexibel und seine Reichweite wird nicht durch Router begrenzt, sprich sie lässt sich erweitern, zB zu einem ausgedehnten WAN.

7.2. Die größten Vorteile von VLAN

Wie sich Kommunikation in VLAN integrieren lässt

Die VLAN-Integration wird in der Regel auf einem Verteiler eingerichtet (nur in besonderen Fällen nimmt eine getaggte Kommunikation den Übertragungsweg eines anderen Geräts). Verteiler, welche VLAN unterstützen, enthalten zumindest ein VLAN. Dies wird standard-mäßig VLAN NO1 bezeichnet, welches sich nicht löschen oder abschalten lässt. Sofern es nicht anders eingerichtet wird, werden alle Ports (sprich die gesamte Kommunikation) in VLAN 1 integriert. Es gibt vier Hauptmethoden, wie sich die Kommunikation in ein VLAN integrieren lässt. In der Praxis kommt jedoch fast nur die erste Methode zur Anwendung.

1. Port-basierte Methode

Ein Verteiler-Port wird manuell und tief in ein bestimmtes VLAN integriert (konfiguriert). Die gesamte Kommunikation, welche über diesen Port stattfindet, gehört zu dem bestimmten VLAN. Das heißt: So lange, bis dem Port ein weiterer Verteiler hinzugefügt wird, werden sich alle damit verbundenen Geräte im selben VLAN befinden. Damit ist es die schnellste und am häufigsten verwendete Methode. Darüber hinaus gibt es keine besonderen Anforderungen, an die VLAN-Integration. Dessen Definition ist in jedem Verteiler lokal-basiert. Darüber hinaus ist diese Methode klar geordnet und leicht zu verwalten.

2. MAC-Adressen basierte Methode

Die Ports werden entsprechend des Ursprungs der MAC-Adresse in das VLAN integriert. Zu diesem Zweck muss eine detaillierte Tabelle erstellt werden, welche eine Liste der MAC-Adressen der einzelnen Geräte enthält – und zwar zusammen mit dem bestimmten VLAN. Der größte Vorteil ist die höchst dynamische Integration: Wird ein Gerät an einen anderen Port angeschlossen, wird es automatisch in das entsprechende VLAN integriert. Es gibt zwei Arten, auf welche sich diese Methode anwenden lässt: Entweder wird die Integration des Ports in das VLAN entsprechend der MAC-Adresse des ersten Frames eingerichtet, womit die Einstellung gleich bleibt, bis der Port abschaltet. Alternativ wird jeder Frame entsprechend der MAC-Adresse extra in das VLAN integriert. Trotzdem ist diese Methode sehr leistungshungrig. Cisco fand jedoch eine Lösung, die VLAN Membership Policy Server (VMPS) genannt wird und welche einen speziellen Server zur Verwaltung von den Tabellen mit MAC-Adressen braucht. Darüber hinaus integriert diese Methode Ports

in das VLAN. Demzufolge müssen – vorausgesetzt, dass mehrere Geräte (max. 20) damit verbunden sind – alle davon im selben VLAN sein.

3. Protokollbasierte Methode (entspricht den Informationen in der 3. Schicht)

Mit dieser Methode wird die protokollbasierte Integration übertragener Pakete festgelegt, zB die Trennung der IP-Operationen von Apple Talk, die IP-Adressen basierte oder raumbezogene Integration. In der Praxis kommt sie jedoch nur selten vor. Ein Gerät benötigt eine streng festgelegte IP-Adresse und der Verteiler muss bis zur dritten Schicht operieren (oft operiert er sogar bis zur zweiten), was zu einer merklichen Geschwindigkeitsreduktion führt.

4. Authentifizierungsmethode

Diese Methode verifiziert einen Nutzer oder ein Gerät mittels IEEE 802.1x-Protokoll und nimmt diese gemäß der bereitgestellten Information ins VLAN auf. Primär handelt es sich um eine Sicherheitsmethode, welche den Netzwerkzugriff regelt (NAC). Wird sie jedoch erweitert, dient sie auch als VLAN. Die Methode ist auch dank ihrer Vielseitigkeit effektiv, sprich weder ein physisches Gerät noch der Verbindungsort sind von Relevanz. Ein RADIUS- Server, welcher die Nutzeridentität verifiziert, erlaubt auch das Zuordnen von VLAN-Nutzern. Im Anschluss an die erfolgreiche Authentifizierung werden diese Informationen gesendet. Diese Methode erlaubt auch eine spezielle Einstellung, welche dafür sorgt, dass ein nicht authenfizierter Nutzer in ein spezielles Host-VLAN eingegliedert wird. Cisco-Verteiler können einen Einzel-Host-Port haben, über welchen nur ein Gerät eine Verbindung herstellen kann. Ebenso gibt es einen Multi-Host, welcher es mehreren Geräten erlaubt, sich an einen Port anzuschließen, wobei sich der Port nach der ersten Authentifizierung selbst authentifiziert, wodurch alle Geräte miteinander kommunizieren können.

7.3. Grundsätze der VLAN-Kommunikation

Im Wesentlichen gibt es zwei Arten der VLAN-Zugehörigkeit: Die erste davon dreht sich um die Kommunikation innerhalb eines Verteilers, die zweite bezieht sich auf die Kommunikation zwischen den Verteilern.

Auf einem Verteiler basierendes VLAN

Die VLAN-Kommunikation innerhalb eines Verteilers ist in der Tat sehr einfach. Der Verteiler behält in seinem Arbeitsspeicher Informationen über eine bestimmte Kommunikation (Port), welche zu einem bestimmten VLAN gehört. Daraus folgt, dass innerhalb eines Verteilers nur ein korrektes Routing erlaubt ist. In so einem Fall werden einzelne Ports in ein VLAN integriert – und zwar entweder statisch oder dynamisch, wie es oben bereits erwähnt wurde (Optionen 2, 3, 4). Cisco bezeichnet diese Ports als Zugangsports.

Auf mehreren Verteilern basierendes VLAN

In der Tat ergibt sich eine deutlich kompliziertere Situation, wenn es zu beachten gilt, dass die Information über eine bestimmte VLAN-Integration nicht im Zuge ihres Transfers zu einem anderen Verteiler verloren gehen darf, sprich das gesamte Netzwerk dasselbe VLAN nutzen soll – und zwar unabhängig von einer bestimmten Verteiler-Gerät-Verbindung. Überdies kann ein Gerät an zwei Verteilern angeschlossen sein, dann in dasselbe VLAN integriert werden und die benötigte Information kann trotzdem übertragen werden. Dieses Verfahren ist jedoch sehr ineffektiv.

8. URL, X/HTML, HTTP

URL ist die Abkürzung für Uniform Resource Locator. Dieser wird verwendet, um Dokumente im Internet eindeutig identifizieren zu können. Ein Beispiel für eine URL-Website ist:

http://www.adaptic.cz/znalosti/slovnicek/url/

Dieses zeigt den Aufbau einer URL: CZ ist die Top-Level-Domain, die Second-Level-Domain ist Adaptic und die Third-Level-Domain ist WWW. Diese werden durch Punkte voneinander getrennt. Darüber hinaus enthält die URL einen Pfad zu einer Website eines Verzeichnisses mit der mit Slashes gegliederten Struktur /znalosti/slovníček/url/. Der letzte Teil der URL ist ein Protokoll, welches die Abfrage des Webseiten-Servers ermöglicht. In diesem Fall handelt es sich um das HTTP-Protokoll, welches ganz am Anfang steht (http://).

Des Weiteren kann die URL folgende Informationen enthalten

- einen Webseiten-Titel mitsamt dessen Endung enthalten (zB index.htm),
- die Port-Nummer, welche den erforderlichen Dienst identifiziert (sie steht nach der Top-Level-Domain und ist durch einen Doppelpunkt getrennt, zB 80),
- sofern benötigt auch Benutzernamen und Passwort (erscheinen nach dem Protokoll – user-name:password:@).
- URL-Tabs, welche sich auf eine bestimmte Stelle auf der Webseite beziehen (scheint als #tab am Ende einer URL auf)
- Website-Parameter (tauchen hinter dem Namen der Website auf und sind durch ein Fragezeichen separiert, zB ?logged=true) können auch ein integraler Bestandteil einer URL sein.

8.1. Arten von URLs

Die Art der im Beispiel oben gezeigten URL nennt man eine **absolute URL**. Es gibt jedoch auch eine **relative URL**, welche sich auf eine bestimmte Stelle eines aktuellen Dokuments bezieht (eine Website, welche ihre Links enthält). In so einem Fall können ein paar Teile ausgelassen werden. Das heißt: Vorausgesetzt, eine referenzierte Webseite befindet sich auf demselben Server, kann die Bezeichnung des Servers (Domain) in dieser bestimmten URL weggelassen werden. Auf der anderen Seite ist es nicht notwendig, einen Pfad in die URL zu schreiben, solange sich die Webseite im selben Verzeichnis wie die referenzierte Webseite befindet.

Eine gut gepflegte URL wird **cool URL** genannt (auch auf Tschechisch). Gesetztenfalls, dass nur die Einsetzbarkeit von Interesse ist, spricht man von einer **nutzerfreundlichen URL**. Geht man auf der anderen Seite davon aus, dass nur Suchmaschinen berücksichtigt werden, ist von einer **seofreundlichen URL** die Rede.

8.2. Die Bedeutung der URL-Gestaltung

Die Form einer URL wirkt sich stark auf deren Sichtbarkeit im und Verwendungsmöglichkeit für das Web aus. Ist ein Domainname zB kurz und prägnant, können sich die Nutzer diesen leichter merken. Darüber hinaus lässt er sich leichter per Telefon diktieren. Enthält eine URL hingegen ein Schlagwort (oder enthalten Teile der URL ein solches), so wirkt sich dies positiv auf deren Auffindbarkeit für eine Suchmaschine aus. Enthält eine URL jedoch eine große Anzahl an Parametern, wirkt sich dies in beiden Fällen negativ aus: URLs, welche in Großbuchstaben geschrieben werden oder sehr lange sind, werden in E-Mails stark gekürzt und das E-Mail-Programm gibt sie unleserlich wieder.

URL

Eine URL wird entweder als eine absolute oder relative Adresse geschrieben. Während die absolute Adresse sich genau mit der URL deckt, bezieht sich die relative Adresse auf einen bestimmten gekürzten Adresseintrag, welcher auf einer Suchmaschine basiert, die den Eintrag der Adresse der aktuellen Website versteht. Zu beachten gilt, dass eine URL auch die Groß-/Kleinschreibung berücksichtigt.

Absolute URL

Jede absolute Adresse besteht aus einem Protokoll und einem Domainnamen. Darauf folgt meist ein Verzeichnispfad und Dateiname. Manchmal enthält die Adresse auch eine Port-Nummer, eine Tab-Bezeichnung und einen Abfrage-String.

Protokolle

HTTP- oder HTTPS-Protokolle übertragen zumeist HTML-Webseiten. Sie werden in Form von http:// und https:// in die URL geschrieben.

Daraus ergibt sich kein allzu großer Unterschied, solange der Server mit der Suchmaschine kommuniziert. Festzuhalten gilt, dass HTTP unverschlüsselt über das Internet übertragen wird, wohingegen HTTPS ein verschlüsseltes Protokoll ist.

In der Tat sollten die beiden Protokolle nicht verwechselt werden, da beide mitunter auf einem bestimmten Server nicht funktionieren könnten. Das heißt: Wann immer absolute Adressen verwendet werden, muss eruiert werden, welche Protokolle in einem bestimmten Web funktionieren.

Domains

Jeder Internetserver hat einen Domainnamen. Dieser besteht aus drei Teilen, welche durch Punkte voneinander getrennt werden:

- Bezeichnung des virtuellen Servers, zumeist www (Third-Level-Domain)
- Bezeichnung der Second-Level-Domain (Registrierung erforderlich)
- Top-Level-Domain, zumeist Länder- oder Firmenkürzel wie CZ, SK oder COM

Port

Auf eine generische Domain folgt selten eine per Doppelpunkt abgegrenzte Port-Nummer.

Verzeichnispfad

Die Zieldatei befindet sich entweder in einem Verzeichnis oder direkt im Hauptverzeichnis des Servers. Verzeichnisse sollten in der URL an die generische Domain angehängt werden. Ein Schrägstrich (kein Backslash) wird vor der Bezeichnung eingefügt. Verzeichnisse mit mehreren Ebenen schreibt man hintereinander und trennt sie durch Slashes voneinander.

Dateien

Ein Dateiname wird nach dem Verzeichnispfad geschrieben (wenn er existiert). Vor dem Dateinamen wird ein Slash eingefügt.

Registerkarte (Tab)

Ein direkter Link stellt eine Verbindung zu einem Tab in einem referenzieren Dokument her. Hierzu schreibt man nach dem Dateinamen eine Raute # sowie den Tab-Namen in die URL.

Anfrage

Eingabedaten für ein bestimmtes Script können auch Teil einer URL sein. Diese werden nach dem Fragezeichen ans Ende der URL geschrieben. Syntax:

```
Name=Wert&Name2=Wert2
```

Beispiel für eine typische absolute URL:

http://www.jakpsatweb.cz/html/url.htm#priklad

Adressteil	Beispiel	Andere mögliche Werte
Protokoll	http://	ftp:// , mailto: etc.
Third-Level-Domain (Server)	www.	www. , xyz.
Second-Level-Domain	jakpsatweb.	seznam. , mujweb. usw.
Top-Level-Domain	cz	com, sk, gov usw.
Port	nichts	:80 , :Zahl
Pfad (Verzeichnisse)	/html/	/, /xyz/Verzeichnis/
Dateiname	url.htm	index.html xyz.html
Registerkarte	#Beispiel	#Registerkartenbezeichnung
Anfragen	nichts	?Variable=Wert

Relatives Adressieren

Oft ist es so, dass das Eintippen einer vollständigen absoluten Adresse ein unnötiger und langwieriger Prozess ist. Man kann sich diesen Aufwand sparen, indem man stattdessen relative Adressen verwendet.

Die Idee der relative Adressen basiert auf bestehenden Dateien, welche miteinander verbunden und auf demselben Server gespeichert sind. Jede Datei, welche eine andere URL-Datei benötigt, hat eine absolute URL. Aus diesem Grund muss nur ein Dateipfad, Slash und Dateiname an die Adresse angehängt werden, woraus sich eine relative URL ergibt.

Relative URL = Pfad/Datei_Name

Verzeichnisse werden durch Schrägstriche voneinander getrennt. Ist es der Fall, dass sich eine Zieldatei höher in der Verzeichnishierarchie befindet (wodurch ein bestimmter „Sprung nach oben“ erforderlich wird), so müssen zwei Punkte als Ersatz für die Bezeichnung des übergeordneten Verzeichnisses eingefügt werden.

Ein Beispiel: Fügt man ein Bild mit dem Logo “Jak psát web” (Wie man ein Web schreibt) auf einer Website ein, so macht man das mithilfe einer relativen Adresse. Dies sieht wie folgt aus: <img src="../images/jakpw.png">

8.3. XHTML

XHTML bezeichnet eine moderne Mark-Up-Sprache, welche die bereits veraltete Sprache HTML ersetzt hat. XHTML-Dokumente können auch unter Anwendung der Sprache XML umgesetzt werden, wovon es sich in mehrerlei Hinsicht unterscheidet. In diesem Kontext sind beispielsweise die Anforderung an die Code-Deklaration, strengere Regeln betreffend Einträge (müssen geschlossen sein) und Attribute (Kleinbuchstaben in Anführungszeichen) zu nennen.

Heutzutage existieren zwei Versionen von XHTML. Die erste davon ist XHTML 1.0, welche sich wiederum in drei Varianten aufteilen lässt. Dies sind: Frameset (für Websites, die Frames verwenden), Transitional (erleichtert die Umwandlung in XHTML) und Strict (die genaueste Variante). Die zweite Version ist XHMTL 1.1. Im Wesentlichen unterscheidet sich diese kaum von der Strict-Variante von XHTML 1.0. Sie ist nur in mehrere Module unterteilt.

Obwohl die Meinungen darüber auseinandergehen, stellt XHTML im Hinblick auf die Umsetzung von WWW-Websites das praktikabelste Werkzeug dar. Anzumerken gilt, dass XHTML 1.1 nicht mit älteren Browsern kompatibel ist. Auf der anderen Seite geben die zwei verbleibenden Varianten von XHTML 1.0 zu wenige Einschränkungen vor, wodurch sie, wie HTML, hohe Anforderungen an die Disziplin der Programmierer stellen.

XHTML unterscheidet sich vom neueren HTML-Standard. Im Großen und Ganzen hat sich HTML lange Zeit nicht weiterentwickelt. Erst in der HTML-Version 4.01 wurde ein erster Annäherungsversuch an XHMTL unternommen.

Das “X” am Beginn von XHTML steht für eXtensible, sprich erweiterbar. In der Praxis jedoch nimmt man es jedoch eher als “einengend” und “beschneidend” wahr.

Insgesamt wird XHMTL von aktuellen Browsern ebenso unterstützt wie HTML (was 2004 geschrieben wurde, ist auch 2012 gültig). Obwohl man zunächst davon ausging, dass XHTML in Zukunft besser unterstützt werden würde als HTML, so ist in Anbetracht der Erfahrung, welche man mittlerweile betreffend die Browser-Entwicklung sammeln konnte, nicht anzunehmen, dass dies tatsächlich der Fall sein wird.

Unterschiede zwischen XHTML und HTML

Anders als in HTML müssen bei XHTML alle Tags – sogar jene, welche keinen End-Tag haben (zB <meta>, <link>, <br>, <hr> or <img>) – geschlossen werden. Der Eintrag kann mehrere Formen haben: entweder klassisch (valide) <img></img> oder abgekürzt <img/> oder geringfügig angepasst <img />. Es wird dennoch davon abgeraten, die erste Methode zu verwenden, wenn ein XHTML-Dokument des Typs text/html verschickt wird. Die zweite Schreibweise, jene ohne Lücke, sollte man nicht für ältere Browsern verwenden, da sie das letzte Attribut auslassen könnten, sofern ein solches eingegeben wurde.

Darüber hinaus muss man in XHTML – anders als bei HTML – alle Tags und deren Attribute in Kleinbuchstaben schreiben. Der Grund dafür ist die Unterscheidung zwischen Groß- und Kleinschreibung in DTD und X(HT)ML, mit welchen diese deklariert und referenziert werden. Mit anderen Worten: Die Schriftgröße wird beachtet. Unter der Voraussetzung, dass man ein eigenes DTD deklariert, ist der Einsatz von Großbuchstaben kein Problem.

Alle Attributwerte müssen in Anführungszeichen gesetzt werden.

Darüber hinaus muss ein Dokument mit einer XML-Deklaration beginnen, obwohl deren Einsatz nicht verpflichtend ist, wenn das Dokument in UTF-8 verschlüsselt ist oder die Verschlüsselung von einem höheren Protokoll übernommen wird (zB HTTPS). [14]

Sofern Frames benötigt werden, kann man ein Dokument als XHTML 1.0 Frameset, bei einzelnen Webseiten sogar XHTML Transitional, deklarieren.

Ein XHTML-Dokument sollte auf eine andere MIME-Art versendet werden als ein gewöhnliches HTML-Dokument. [15]

8.4. HTTP

HTTP bezieht sich afu ein Internetprotokoll, welches ursprünglich für den Austausch von Hypertext-Dokumenten zwischen einem Server und einem Browser (sprich WWW-Dienst) konzipiert wurde. In der Tat ist die aktuelle HTTP-Version in der Lage, Dateien jeglicher Art zu übermitteln und sie wird auch für mehrere Zwecke genutzt (zB die Fernbedienung von Anwendungen). Es gibt auch eine sichere Version von HTTPS für HTTP.

HTTP basiert auf dem Prinzip Anfrage Antwort. Individuelle Anfragen sind aus der Sicht des Servers nicht erkennbar. Deshalb wird HTTP auch als zustandsloses Protokoll bezeichnet. Tatsächlich war dies ein großer Vorteil in Zeiten von Internetauftritten. Programmiert man jedoch komplexere Web-Anwendungen, treten vertrackte Probleme auf. So lässt es HTTP zB nicht zu, dass man den Inhalt eines Warenkorbs in einem Online-Shop speichert. Daraus folgt, dass man effektivere Methoden benötigt, um das Problem in den Griff zu bekommen, zB Cookies.

HTTP-Protokoll

Ein HTTP-Protokoll erschließt einen Kommunikationsweg des Browsers zum Server, während eine Website heruntergeladen wird.

Effektiver Einsatz von HTTP

Um eine Website zu erzeugen, ist es nicht notwendig, Kenntnis über das HTTP-Protokoll zu haben. Sobald es jedoch um komplexere Angelegenheiten geht oder man sich mit einer Suchmaschinenoptimierung auf fortgeschrittener Ebene beschäftigen muss, benötigt man ein tieferes Verständnis von den Aktivitäten, welche zwischen dem Server und dem Client stattfinden.

HTTP-Header stellen zB Informationen über Weiterleitungen, Caching, Cookies, Referrer und Komprimierungen zur Verfügung.

Sobald Scripts oder komplexere Web-Programme geschrieben werden, ist es von Vorteil zu wissen, wohin und wie man eine bestimmte HTTP-Antwort sendet.
Die Abkürzung HTTP steht für Hyper Text Transfer Protocol (Hypertext ist ein Text mit Links).

Funktionsweise des HTTP-Protokolls

Ein Client kommuniziert mit dem Server, sprich der Client will etwasund der Server stellt es zur Verfügung.

- Ein Client wird in der Regel durch einen Internet-Browser (Explorer, Mozilla, Opera) repräsentiert. Ein Suchroboter oder ein anderes Programm können das jedoch auch.
- Ein HTTP-Server enthält ein Programm, welches in einem Server-Bereich auf einem Computer läuft (obwohl ein Computer auch “Server” genannt wird, ist damit nicht der “HTTP-Server” gemeint). Der häufigste HTTP-Server ist das Programm Apache.

Das HTTP-Protokoll ist somit eine Art von Sprache, mit deren Hilfe die zwei Programme miteinander kommunizieren. Dies geschieht über ein Netzwerk, meistens das Internet.

Ein Client benötigt in der Regel eine bestimmte Website. Er verbindet sich mit einem Server und fragt den Server nach URL-Webseiten. So eine Anfrage wird im HTTP-Protokoll formuliert (die Verbindung selbst wird über das TCP-Protokoll hergestellt). Daraufhin stellt der Server die Anfrage zu und sendet eine Antwort zurück, welche ebenfalls im HTTP-Protokoll festgeschrieben ist. So sendet er zB HTTP-Header an einen Client, gefolgt von einem Webseiten-Text in HTML. Der Client erhält die Antwort, liest die Header und zeigt die Website an.

Beispiel einer HTTP-Kommunikation

Ein Leser möchte eine Website anschauen. Ihre URL lautet wie folgt:

https://www.jakpsatweb.cz/server/http-protokol.html.

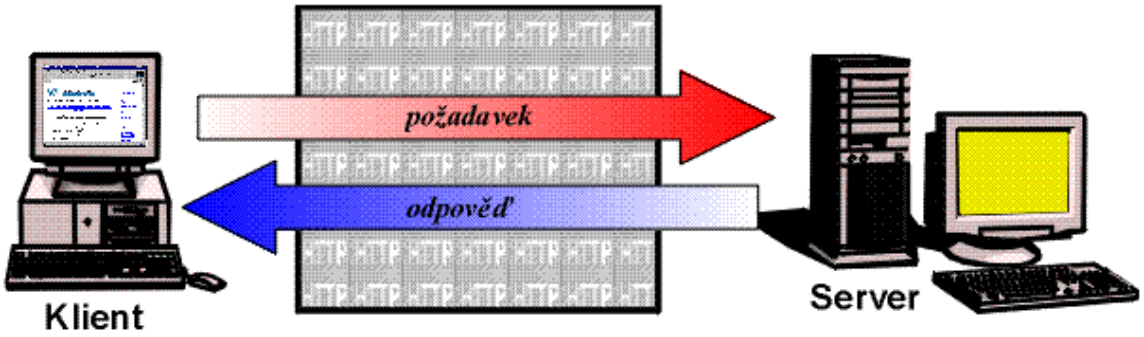
1. Der Leser tippt die URL in den Browser ein.
2. Der Browser (Client) evaluiert die Domain und findet via DNS heraus, nach welcher IP-Adresse gefragt werden soll.
3. Der Client stellt via TCP-Protokoll eine Verbindung zum unter der ermittelten IP-Adresse befindlichen Server her. Hier kommt HTTP ins Spiel.
4. Der Browser sendet folgenden HTTP-Befehl an den Server:

GET /server/http-protokol.html HTTP/1.1
HOST: www.jakpsatweb.cz

HTTP-Protokolle

Der Dienst des World Wide Web basiert im Wesentlichen auf drei Technologien: HTML, URL und http. HTML bezeichnet eine Mark-Up-Sprache, die für die standardmäßige Beschreibung des Inhalts und der Struktur einer Website verwendet wird. URL steht im Zusammenhang mit bestimmten Adressen, welche im Web verwendet werden: Jede Website hat ihre eigene, eindeutige Adresse in Form einer URL. HTTP, das Hypertext Transfer Protocol, ist jenes Protokoll, welches für die Kommunikation zwischen Browsern und Web-Servern verwendet wird. Mit seiner Hilfe werden die vom Benutzer gewünschten URL-Webseiten (über einen Browser) vom Server übertragen. Der Server wiederum schickt per HTTP eine Website an den Benutzer zurück, welche in HTML geschrieben wurde.
Um die Prinzipien von CGI-Skripten zur Gänze zur verstehen, ist zumindest ein rudimentäres Wissen über HTTP erforderlich. Aus diesem Grund werden die Hauptmerkmale von HTTP nachfolgend im Detail angeschaut.

Das HTTP-Protokoll ergibt sich aus der Client/Server-Architektur. Der Client, in diesem Fall ein Browser, verbindet sich mit dem Server und schickt eine Anfrage. Im Gegenzug erhält er eine Antwort vom Server. Das standardmäßige Format von Anfrage und Antwort ist im HTTP-Protokoll festgelegt. Verkompliziert wird das ganze dadurch, dass es drei Protokoll-Versionen gibt: 0.9, 1.0 and 1.1. Daraus folgt, dass sich das Format von Anfrage und Antwort in einzelnen Versionen grundlegend unterscheidet.



Anfrage Antwort

Abb.: Der Kommunikationsablauf zwischen Client und Server

Haupteigenschaften von HTTP

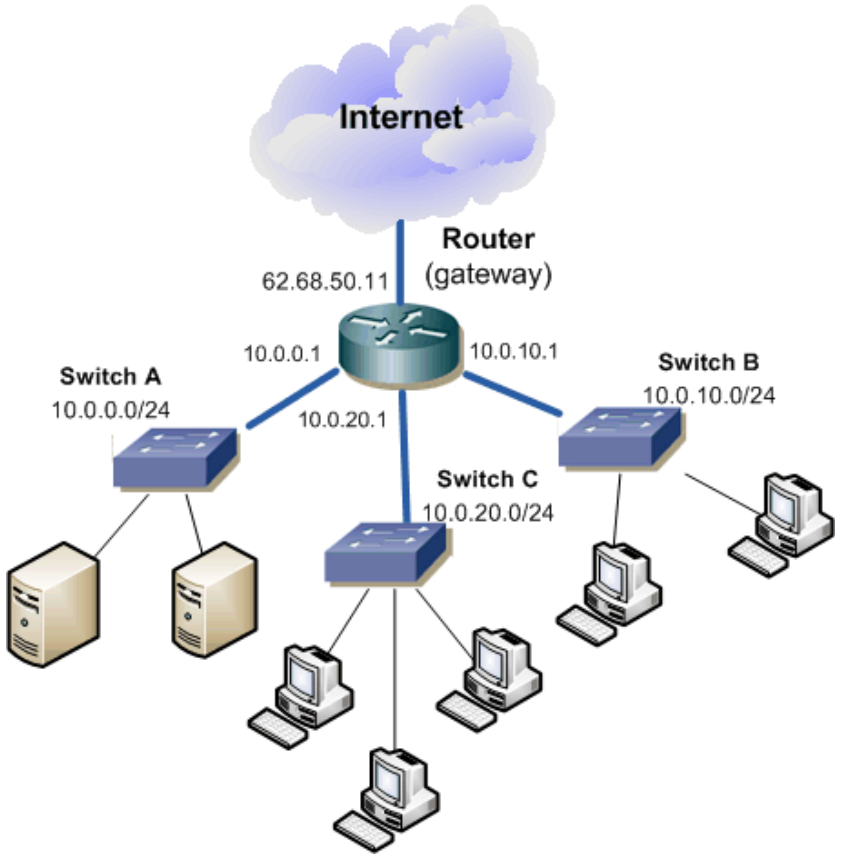
Um dieses Kapitel zur Gänze zu verstehen, ist ein umfassendes Wissen über die Hauptmerkmale von HTTP erforderlich, sprich über die tatsächliche Funktionsweise des Protokolls. HTTP bezieht sich auf die Anwendungsebene verteilter Hypermedia-Informationssysteme. Das heißt, dass dieses Internetprotokoll in der Regel nicht nur für die Datenübertragung zwischen Client und Server verwendet wird, sondern noch eine Reihe weiterer Aufgaben übernimmt. Da HTTP zustandslos ist, unterscheidet es nicht zwischen Clients, von welchen es Anfragen erhält. Sendet beispielsweise ein Client zwei Anfragen gleichzeitig, wird der Server nicht erkennen, dass es sich um denselben Client handelt.

HTTP existiert in drei Versionen: 0.9, 1.0 und 1.1. Die erste davon, welche HTTP/0.9 bezeichnet wird, ist ein einfaches Protokoll, welches in der Lage ist, Daten im Internet eingeschränkt zu übertragen. HTTP/1.0 hingegen erlaubt dem Protokoll, Informationen im MIME-Format zu übertragen, wodurch Daten auch Meta-Informationen enthalten können. Gesamt gesehen wurde die größte Verbesserung jedoch dadurch erreicht, dass alle Verbindungen dauerhaft gemacht wurden. Dies geschah in HTTP/1.1, der bislang aktuellsten Version. Dauerhaft heißt, dass eine Verbindung nicht geschlossen wird, bis ein Teil des Client-Server-Paars einen Beendigungs-Header verschickt. Zuvor beendete HTTP eine Verbindung automatisch nach jeder einzelnen Server-Antwort. Durch diese große Verbesserung hat sich die Übertragungsgeschwindigkeit massiv erhöht, da der Server nicht für jedes Bild, Applet und Frame eine neue Verbindung herstellen muss.

9. ROUTINGPROTOKOLLE

Routing bezeichnet eine Methode, welche sich auf das Verknüpfen einzelner Netzwerke fokussiert (Subnetze). Das ursprüngliche Gerät, welches für das Routing konzipiert wurde, war der Router. Heutzutage werden hierzu jedoch hauptsächlich L3-Verteiler, Firewalls oder einfach Server/Computer eingesetzt. Ein Router leitet die Kommunikation von einem Netzwerk an ein anderes weiter.

Die nachfolgende Abbildung illustriert ein einfaches Netzwerk-Beispiel mit den Subnetzen A, B und C. Diese Subnetze sind durch einen Router miteinander und dadurch mit dem Internet verbunden. Daraus lässt sich Folgendes ableiten: Möchte beispielsweise Subnetz B mit dem Subnetz-Server A kommunizieren, sendet dieses Daten an den Router, wodurch deren Auslieferung an Subnetz A sichergestellt wird. Möchte die Station über das Internet kommunizieren, sendet der Router die Daten an eine andere Schnittstelle.



Die Einteilung von Netzwerken in Subnetze basiert auf einer bestimmten Hierarchie, wobei alle Verknüpfungen einen Router haben müssen. Die Kommunikation erfolgt nach oben hin, sprich in die nächstgelegene Schicht, welche bestimmte Subnetze miteinander verbindet, von wo aus sie wieder nach unten verlegt wird. Die Pfadlänge wird in Form von **Hops (Sprüngen)** berechnet, womit einzelne Transite von Gerät zu Gerät gemeint sind, sprich die Anzahl von Routern, welche sich auf dem Weg befinden, ergänzt um die Zahl 1.

Eine direkte Verbindung zwischen zwei Computern entspricht einem Hop. Der Begriff **„nächster Hop“** wird auch häufig verwendet und bezieht sich auf die Adresse des nächsten auf dem Weg gelegenen Routers.

Die nächste Abbildung illustriert die oben erklärte Situation. Es gibt einen kleinen Abschnitt (nur schematischer Natur) eines größeren Netzwerks oder des Internets. Kleinere Router befinden sich in den Blättern des Baums und sind mit Verteilern und Computern verbunden. Diese Router sind mit anderen (größeren) Routern auf unterschiedlichen Ebenen verbunden. Es ist jedoch so, dass größere Router für gewöhnlich nur die Aufgabe haben, das Netzwerk vor einem Ausfall zu schützen oder die Last zu verteilen.

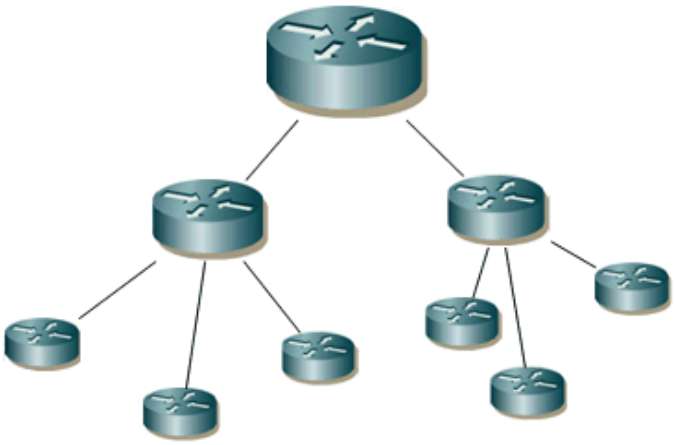


Abb.: Router-Hierarchie im Netzwerk?

9.1. Routing: Technische Begriffe

Router
Ein Gerät, welches das Routing durchführt.

Routing
Der Prozess der Datenweiterleitung zwischen Netzwerken.

Route
Ein angewendeter Pfad, welcher in einer Routing-Tabelle festgeschrieben ist.

Routing-Tabelle
Enthält Aufstellungen über einzelne Routen.

Routing-Protokoll
Verwaltet die Ausrichtung eines gerouteten Protokolls: Es legt die beste Route hin zum Ziel fest und sendet Routing-Informationen an andere Router.

Geroutetes Protokoll
IP, IPX oder Apple Talk. Auch ein wichtiger und häufig verwendeter Begriff.

Router on Stick
Dieser Begriff bezeichnet einen Router, welcher über einen Hauptanschluss mit einem Verteiler verbunden ist. Das bedeutet, es sind nur ein Router und eine Leitung verfügbar, was zu einer beträchtlichen Belastung dieser beiden führt, wodurch letztlich Probleme (Ausfälle) hervorgerufen werden.

Einteilung von Routing-Protokollen
Die Routing-Tabelle enthält einige Aufzeichnungen von Routen, welche unterschiedlichen Ursprungs sein können. Daraus folgt, dass Pakete auf einer der folgenden Routing-Arten geroutet sind:

- Statisches Routing: manuell eingetragene Routen (Aufzeichnungen in der Routing-Tabelle), sicher und von hoher Qualität. Veränderungen in der Netzwerk-Topologie spiegeln sich darin jedoch nicht wieder.

- Dynamisches Routing: Das Netzwerk passt sich automatisch an Veränderungen in der Topologie und beim Transport an. Routen werden automatisch von einem Routing-Protokoll berechnet.

- Standardmäßiges Routing: Solange keine andere Art festgelegt wurde, kommt dieses zum Einsatz.

Dynamische Routing-Protokolle lassen sich wiederum in zwei Arten unterteilen:

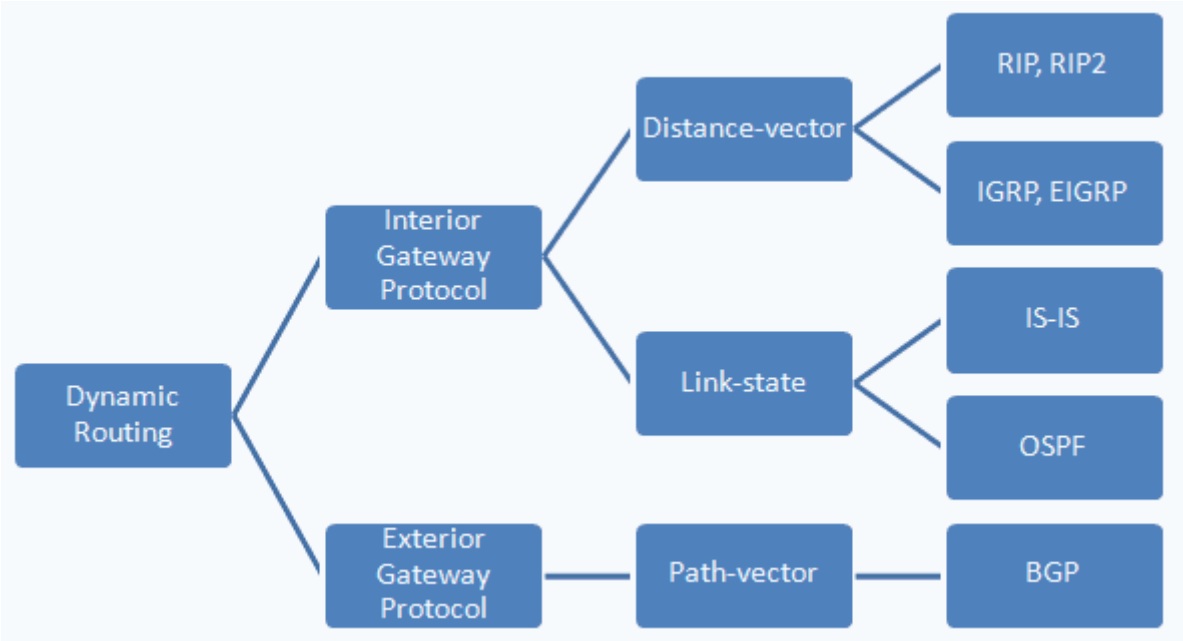
- Distanzvektoralgorithmus: Router behalten die Routing-Tabelle bei, welche Informationen über die Distanz (Vektor) eines bestimmten Netzwerks enthält. Darüber hinaus senden sie die Routing-Tabelle an ihre Nachbarn, welche ihrerseits eine eigene Routing-Tabelle erstellen und diese weiterleiten. Um die bestmögliche Route zu berechnen, werden eine (Anzahl der Hops beim RIP) oder mehrere Mess-größen (Leitungsdurchsatz und IGRP-Verzögerung) verwendet. Zusätzlich wird ein aufgewerteter Typ des Distanzvektorprotokolls in Form eines Pfadvektorprotokolls dargestellt.

- Link-State Routing-Protokoll: Router behalten eine umfassende Netzwerktopologie-Datenbank bei (erstellt mittels LSA), verändern Link-State-Advertisements (LSA). LSAs werden durch ein bestimmtes Ereignis im Netzwerk ausgelöst. Dieses Protokoll verschickt auch Hello-Pakete, welche Informationen über das Protokoll enthalten und reagiert schnell auf Veränderungen in der Topologie. Gleichwohl dehnt es sich auf einen größeren Bereich aus und verwendet mehr Ressourcen des Routers. Darüber hinaus ist seine Messgröße komplex-basiert und die bestmögliche Route wird vom Dijkster-Algorithmus Shortest Path First (SPF) berechnet.

Anmerkung: Es gibt noch eine weitere Art von dynamischem Routing-Protokoll, welche zwar auf dem Distanzvektorprotokoll basiert, jedoch auch einige Merkmale des Link-State-Protokolls besitzt. Hierbei handelt es sich um ein hybrides Routing-Protokoll oder ein fortgeschrittenes Distanzvektorprotokoll. Dessen einziger Vertreter ist das EIGRP.

Darüber hinaus lassen sich dynamische Protokolle dahingehend unterteilen, ob sie für einen Einsatz in einem lokalen Netzwerk konzipiert sind (genauer gesagt in einem autonomen System [AS], welches aus mehreren LANs bestehen kann) oder ob sie netzwerkübergreifend operieren (mehrere AS miteinander verbinden).

- Interior Gateway Protocol (IGP): Routing innerhalb Autonomer Systeme (AS)
- Exterior Gateway Protocol (EGP): AS-übergreifendes Routing



10. SICHERHEIT UND VERSCHLÜSSELUNG

10.1. Netzwerksicherheit

Gefahren:

Lauschangriff, Veränderung übertragener Daten, unautorisierter Zugriff auf ein lokales Netzwerk.

Adäquater Schutz:

- Schutz von Daten vor unautorisiertem Erbeuten, Austauschen und Löschen
- Rechenkapazität einzelner Netzwerkknoten
- Zurückfahren der Funktionalität oder Reduktion von Störungen des Dienstverkehrs

Passive Angriffe

- "Lauschangriff", um nicht-öffentliche Informationen zu bekommen, welche missbraucht werden könnten.
- Verkehrsüberwachung: Analyse der Kontakte, welche über ein Netzwerk erfolgten

Aktive Angriffe

- Datenveränderung
- Einschleusen gefälschter Daten
- Vor aktiven Angriffen kann man sich zwar nicht zu 100% schützen. Im Gegensatz zu passiven Angriffen lassen sie sich jedoch einfacher aufdecken.

Ziele von Sicherheitsdiensten

- Sicherstellung der Geheimhaltung von Daten: Durch das Verschlüsseln des gesamten Kommunikationskanals oder ausgewählter sensibler Daten.
- Sicherstellen, dass sich alle Netzwerknutzer authentifizieren müssen (Aufspüren eines getarnten Eindringlings)
- Sicherstellung der Datenintegrität
- Gewährleisten, dass Mitteilungen verweigert werden können: So wird es Nutzern unmöglich gemacht, das Senden und den Empfang einer Nachricht zu leugnen.
- Vergabe von Zugangsrechten, um den Zugriff auf Computer, Daten und Anwendungen zu kontrollieren. Das Identifizieren und Authentifizieren von Anwendern vor deren Zugriff sind ebenfalls ein integraler Bestandteil dieser Vorkehrung.

- Gewährleisten der Verfügbarkeit von Netzwerkdiensten. Angriffe auf die Verfügbarkeit von Diensten können durch Authentifizierung und Verschlüsselung verhindert werden.

10.2. Firewall

- Bezeichnet eine Reihe von Maßnahmen (implementiert durch HW und SW), welche das Netzwerk vor einem unautorisierten Zugriff von außen schützen und gleichzeitig vor einem Informationsleck bewahren.

- Erlaubt zB die Regulierung des Nutzerzugriffs von externen und internen Netzwerken aus, Die Vergabe von Zugriffsrechten, das Herausfiltern gefährlicher Dienste, das Kanalisieren Der Sicherheit auf einen Kommunikationsknoten, das Blockieren eines feindlichen Mappings des internen Netzwerks sowie das Überprüfen legaler und illegaler Operationen.

- Schützt beim Einstieg ins und Ausstieg aus dem Netzwerk.

- Fungiert als Filter, sprich entscheidet, was und bis zu welchem Punkt etwas erlaubt ist.

10.3. Verschlüsselung

1. Symmetrische Verschlüsselung

Zur Ver- und Entschlüsselung benötigt man einen einzigen Schlüssel. Die symmetrische Verschlüsselung, manchmal auch „gewöhnliche“ Verschlüsselung genannt, bezeichnet einen kryptografischen Algorithmus, welcher einen einzelnen Schlüssel für die Ver- und Entschlüsselung verwendet. Dadurch unterscheidet er sich von asymmetrischen Algorithmen, welche ein Schlüsselpaar verwenden, das aus einem geheimen und einem öffentlichen Schlüssel besteht.

Der große Vorteil symmetrischer Verschlüsselung ist ihre geringe Berechnungskomplexität. Asymmetrische Algorithmen können bis zu einige hundert Mal langsamer sein. Andererseits besteht der größte Nachteil darin, den geheimen Schlüssel teilen zu müssen. Aus diesem Grund müssen sich der Absender und der Empfänger einer geheimen Nachricht auf einen bestimmten geheimen Schlüssel einigen.

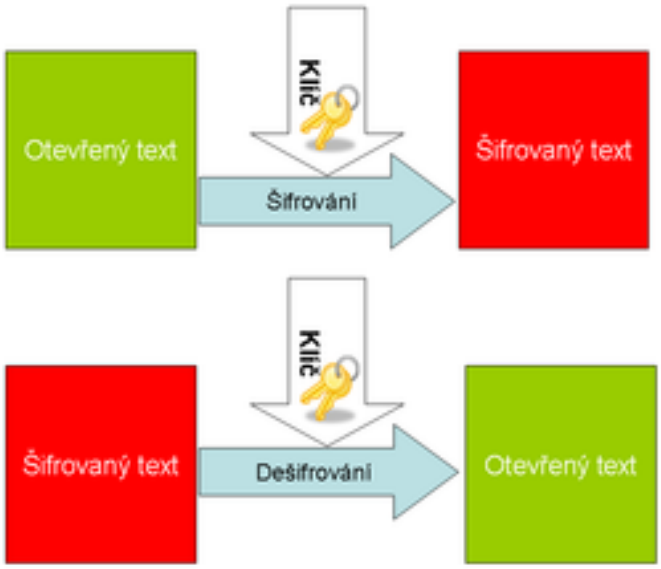


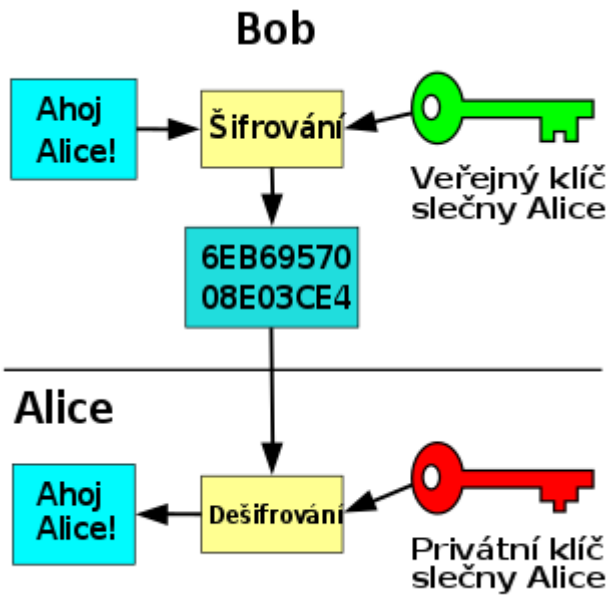
Abb.: Symmetrische Verschlüsselung

Klartext → Verschlüsselung→ verschlüsselter Text

Verschlüsselung → entschlüsseln → Klartext

2. Asymmetrische Verschlüsselung

Beispiele für asymmetrische Verschlüsselung
Asymmetrische Verschlüsselung (Public Key Encryption) bezieht sich auf eine Gruppe von kryptografischen Methoden, die unterschiedliche Schlüssel für das Ver- und Entschlüsseln verwenden. Alles in allem ist dies der Hauptunterschied zur symmetrischen Verschlüsselung, welche nur einen einzigen Schlüssel zum Ver- und Entschlüsseln verwendet.
Die asymmetrische Verschlüsselung nicht nur dazu genutzt, eine geheime Kommunikaion zu gewährleisten, sondern auch für die elektronische Signatur, sprich zur Kenntlichmachung des Verfassers von Daten.



Bob
Hallo, Alice → Verschlüsselung ← öffentlicher Key von Alice

Alice
Hallo, Alice ← Entschlüsselung ← privater Schlüssel von Alice

Abb.: Asymmetrische Verschlüsselung

Der Verschlüsselungsschlüssel bei der asymmetrischen Verschlüsselung besteht aus zwei Teilen: Der erste Teil wird für die Verschlüsselung von Nachrichten verwendet (der Empfänger der Nachricht muss diesen nicht kennen). Der zweite Teil wird zum Entschlüsseln verwendet (der Absender der verschlüsselten Nachricht kennt diesen in der Regel nicht). Klarerweise muss der Absender in diesem Fall keinerlei Geheimnisse mit dem die Botschaft entschlüsselnden Empfänger teilen, weshalb es nicht nötig ist, Schlüssel auszutauschen. Das ist der Hauptvorteil der asymmetrischen Verschlüsselung.

In ihrer gängigsten Variante verwendet die asymmetrische Verschlüsselung einen privaten und einen öffentlichen Schlüssel. Der Schlüssel zur Verschlüsselung ist öffentlich und sein Besitzer stellt diesen zur Verfügung, damit jeder bestimmte Nachrichten verschlüsseln kann. Der Schlüssel zur Entschlüsselung hingegen ist privat, sprich sein Besitzer hält ihn geheim und verwendet ihn, um die Nachrichten zu entschlüsseln (es gibt noch andere Methoden der asymmetrischen Verschlüsselung, welche es erfordern, den Schlüssel geheim zu halten).

Klarerweise müssen der Verschlüsselungs-Schlüssel “e” und der Entschlüsselungs-Schlüssel “d” mathematisch miteinander verflochten sein. Im Hinblick auf die Effektivität der Verschlüsselung ist es jedoch unmöglich, den Entschlüsselungs-Schlüssel aus dem Schlüssel zur Verschlüsselung zu berechnen.

Sicherheit von Computernetzwerken

In diesem Fall bezeichnet der Begriff "Netzwerk" ein System aus mehreren Rechensystemen. Nutzer greifen über eines dieser Systeme auf das Netzwerk zu.

- **Teilen:** Viele Personen können potentiell auf das Netzwerk zugreifen. Diverse Geräte können von nicht notwendigerweise gesicherten Systemen kontrolliert werden.

- **Komplexität:** Im Netzwerk laufen diverse Betriebssysteme, die über Verbindungs-mechanismen miteinander kommunizieren, welche die Sicherheit gewährleisten sollten. So ein Mechanismus muss jedoch ziemlich allgemeingültig sein. Darüber hinaus kann nicht das Netzwerk in seiner Gesamtheit einer Prüfung oder einer Zertifizierung unterworfen werden.

- **Unbekannter Umfang:** Es sind nicht alle verbundenen Personen bekannt. Darüber hinaus ist nicht klar, wie andere Geräte funktionieren.

- **Menge angreifbarer Stellen:** Man kommt nicht umhin, den Sicherheitsmechanismen in allen Geräten zu vertrauen, da sich viele Netzwerkteile außerhalb der Kontrolle des Betreibers befinden.

- **Unbekannter Pfad:** In den meisten Fällen ist es nicht möglich, den Pfad der Datenübertragung zu kontrollieren. Daher kann ihn im Prinzip jeder ohne vorherige Information abfangen. Trotzdem lässt sich die Kommunikation folgendermaßen schützen:

    - <u>Datenfluss:</u> wird auch als "Stromverschlüsselung" bezeichnet. Darunter versteht man die Verschlüsselung von Daten auf eine Art und Weise, die den Eindruck eines sehr zuverlässigen Kommunikationskanals im Hinblick auf einen möglichen Angriff vermittelt.

    - <u>Individuelle Nachrichten:</u> entsprechen einer heutzutage modernen freien Bindung mittels "Messaging". Anwendungsnachrichten werden verschlüsselt oder die Verschlüsselung des Datenstroms wird entweder zwischen zwei Netzwerkknoten oder zwei Anwendungen, welche auf diesen Netzknoten laufen, vorgenommen. Im Hinblick auf die Link-Verschlüsselung gibt es zu sagen, dass die Daten direkt vor dem Eingang in das Kommunikationsmedium verschlüsselt und direkt nach ihrer Ankunft auf dem zweiten Computer wieder entschlüsselt werden. Diese Verschlüsselung findet auf der Ebene der Bitübertragungs- oder Sicherungsschicht des Referenzmodells statt. Der Hauptvorteil ist, dass der Mechanismus für den Nutzer äußerst transparent ist. Darüber hinaus lässt er sich sehr schnell und einfach mit anderen Geräten verbinden.

Ende-zu-Ende-Verschlüsselung

Diese gewährleistet kryptografischen Schutz während des Transferprozesses. Diese Art der Verschlüsselung findet auf der Ebene der Anwendungs- oder Darstellungsschicht des Referenzmodells statt. Diese Verschlüsselung ist jedoch nicht mehr transparent und muss, um wirklich effektiv zu sein, auf geeignete Weise in das gesamte System integriert werden. Ihr Hauptvorteil besteht darin, dass es nicht nötig ist, die gesamte Kommunikation zu verschlüsseln. Es reicht, sensible Daten zu verschlüsseln. Anders als die Link-Verschlüsselung stellt diese Art Authentifizierungs- und Integritätprüfungen zur Verfügung (Ende-zu-Ende). Manchmal werden beide Methoden gleichzeitig verwendet: Die Link-Verschlüsselung für den üblichen präventiven Datenschutz und die Ende-zu-Ende-Verschlüsselung, um den qualitativ hochwertigen Schutz sensibler Daten sicherzustellen. Im Zusammenhang mit der Verschlüsselung ist Folgendes unabdingbar:

- Distributionsmechanismen
- die Verwaltung notwendiger Verschlüsselungsschlüssel,
- kompetente Instanzen zur Sicherstellung des Systembetriebs des kryptografischen Schutzes sowie geeignete kryptografische Geräte, welche grundlegende Funktionen kryptografischen Schutzes bieten.

Abgesehen von den üblichen Problemen der Zugriffsregulierung können sich noch andere heikle Angelegenheiten ergeben.

Abgestufte Zugriffsrechte

Es kann sein, dass der Zugang zu sensiblen Daten nur ein paar Netzwerkknoten vorbehalten ist. Versucht in so einem Fall, ein autorisierter Nutzer von einem anderen Netzknoten aus einen Zugang zu bekommen, können seine Zugriffsrechte massiv beschränkt werden oder der Zugang zu den Daten wird ganz verweigert. Nachdem es den Abruf erhalten hat, beginnt das stille Modem nicht sofort mit der Generierung, sondern wartet, bis die andere Seite zu „verhandeln“ versucht. Folglich ist der Zugriff bis zu einem gewissen Maß auf jene Nutzer beschränkt, welche wissen, dass man sich mit der Leitungsführung des Computers auseinandersetzen muss. Darüber hinaus beschränkt diese Methode die Möglichkeit einer willkürlichen Platzierung dieses Ports. Im Falle eines IP-Protokolls könnte ein Service, welcher auf einem bestimmten Gerät verfügbar ist, welches sich auf einem anderen Port als üblich befindet, eine Alternative zu einem stillen Modem sein.

II. PEER-TO-PEER NETZWERKE

In den letzten 10 Jahren gewannen Austauschnetzwerke, welche auf dem Peer-2-Peer-Prinzip basieren, im Bereich des Datei-Downloads aus dem Internet an Bedeutung. Heute ist das beliebteste das BitTorrent-Protokoll-Netzwerk, welches zig Millionen Nutzer und dutzende Clients (µTorrent, Vuze/Azureus) hat. Darüber hinaus ließ sich in den letzten fünf Jahren der Siegeszug öffentlich zugänglicher kommerzialisierter Web-Server zum Filesharing (Filehosting) beobachten, unter welchen Rapidshare.com der beliebteste ist. Zu dieser Art von Netzwerk lassen sich jedoch auch Systeme zählen, wo mehrere Nutzer an einem Dokument arbeiten oder Dateien synchronisieren (zB Google Docs, Dropbox usw.).

Peer-to-Peer Netzwerke

Der Begriff Peer-to-Peer Netzwerk (P2P) ist sehr allgemein gehalten. Darunter fallen alle Netzwerke, in welchen es eine symmetrische Kommunikation oder Interaktion zwischen Computern gibt (jeder davon kann diese selbst initiieren oder auf Grundlage einer externen Initiierung/Aufforderung die notwendigen Transaktionen und Operationen durchführen). Deshalb ist es nicht möglich, seine Netzknoten funktionell in die zwei üblichen Arten zu unterteilen, sprich in Clients und Server. Dementsprechend fehlt eine grundlegende Aufgabe des Servers. Daraus folgt, dass eine hybride, universelle Art von Computernetzknoten gebildet wird, welcher „Servent" genannt wird (auch wenn der Begriff „Client" häufig dafür verwendet wird). Die Dezentralisierung des Internets, welche im Zeitalter von Usenet (1979) und Fidonet (1984, BBS Systeme) begann, wurde letztlich durch P2P-Netzwerke erreicht. Die Gleichwertigkeit aller Computer in diesem Netzwerk bedeutet jedoch nicht, dass alle Netzknoten dieses Netzwerks homogen sind, was die quantitativen Parameter wie Verbindungs-geschwindigkeit, Menge geteilter Daten, lokale Konfiguration, Verarbeitungsgeschwindigkeit usw. anbelangt.

Im Großen und Ganzen ist die Marke P2P mittlerweile fast zu einem Gattungsnamen für internetbasierte Austauschnetzwerke geworden (sprich für Filesharing-Systeme), obwohl es eine Reihe anderer Anwendungsarten gibt, welche nach demselben Prinzip funktionieren können, zB Anwendungen für dezentralisierte Berechnungen, die Nachrichtenverbreitung, Sprachkommunikation und Chat (IRC, Skype, Qnext, DKMessenger) oder P2P-Übertragung des Programms von Radio- und TV-Stationen im Internet.

Nun ist es jedoch so, dass beliebte P2P-Netzwerke (Filesharer) von den Medien zumeist mit Piraterie in Verbindung gebracht werden. Dies mag zum Teil auch stimmen. Dabei darf man jedoch nicht vergessen, dass zB das BitTorrent-Netzwerk auch stark dafür genutzt wird, große Programme und Datenmengen auf legale Weise zu verbreiten (zB LINUX). Darüber hinaus gibt es Torrent-Kataloge und –Tracker, welche dabei helfen, ausschließlich legales Material (zB Filme) zu verbreiten und zu registrieren – und zwar in gemeinfreier Qualität (http://www.legittorrents.info/, http://beta.legaltorrents.com/, http://www.jamendo.com/, http://www.publicdomaintorrents.com/,); sprich welche aus rechtlicher Sicht kostenfrei genutzt werden dürfen.

Ein Unterscheidungsmerkmal von P2P-Austauschnetzwerken ist, dass alle Dateien oder Text-nachrichten, die auf einem Computer gespeichert sind, welcher mit dem Internet verbunden ist (und mit einem laufenden Client/Server eines bestimmten Netzwerks ausgestattet ist), innerhalb dieser Netzwerke geteilt werden können. Auf der anderen Seite unterscheiden sich die Netzwerke technisch in Bezug auf den tatsächlichen Grad funktioneller Symmetrie, sprich ihre Homogenität und Dezentralisierung und ihrer relativen „Anonymität". Es ist so, dass es so etwas wie vollständige Anonymität im Internet praktisch nicht gibt. Verschiedene Generationen dieser Netzwerke unterscheiden sich nach den oben genannten Merkmalen.

11.1. Generationen von P2P-Netzwerken

Zur ersten Generationen gehören Netzwerke, welche Datei-/Computerlisten sowie Datei- und Computeradressen auf einem oder mehreren zentralen Spezialservern speicherten (Napster, OpenNap, chat – IRC [seit 1988]/IRC@find, Soulseek – das bislang neueste Werk, welches von einer kleineren Community von Musik-Fans genutzt wird). In Bezug auf deren weitere Entwicklung lässt sich sagen, dass die ältesten P2P-Netzwerke für einige ihrer Aktivitäten eine zentralisierte Struktur der Art Client/Server nutzen. Diese beschäftigt sich vor allem mit der Netzwerkverbindung und der Suche nach Ressourcen (Dateien). Aus diesem Grund braucht man keine Server für das routinemäßige Kommunizieren und Teilen zwischen Ende-zu-Ende-Clients. Solche Aufgaben übernehmen Peer-2-Peer-Netzwerke.

Netzwerke der zweiten Generation sind heutzutage die am häufigsten verwendeten. Zentrale Server fehlen komplett: Gleichwohl basieren diese Netzwerke in der Regel nicht auf vollkommen gleichwertigen Servent-Netzknoten, sprich Computer können nicht im großen Stil durch andere Computer ersetzt werden (nur bei Vertretern wie Gnutella oder Freenet). In der Tat wird die perfekte Symmetrie in den Peer-to-Peer-Regeln in der Praxis oft reduziert, um die Effektivität und Zuverlässigkeit der Suche zu erhöhen oder das Identifizieren von Dateien zu erleichtern und somit deren Downloadgeschwindigkeit zu erhöhen.

Heutige P2P-Systeme sind durch "lokale-zentrale" oder speziell abgestellte/zweckbestimmte Komponenten gekennzeichnet, wie zB verschiedene "Super-Netzknoten" (FastTrack-Netzwerk mit Clients wie Kazaa), Netzknoten (DirectConnect, DC++) oder Suchmaschinen und Indexierer (OpenFT), aus denen alle (auf freiwilliger Basis) einzelne Computer werden können. Diese speziellen „Super-Netzknoten" sind wichtig für deren schnelle Verbindung und das Katalogisieren aller anderen gewöhnlichen Computer-Knoten und ihrer Ressourcen. Sie verhindern auch das Auftreten von „Flaschenhälsen" innerhalb von Datenströmen. Die weiteren "asymmetrischen" Komponenten bezeichnen spezialisierte Speicher-Server, welche digitale Hash-Abbilder einzelner Dateien bereitstellen (Identifizierungssignatur, zB Torrents wie bei BitTorrent, Magnetstreifen wie bei Gnutella, ed2k wie

bei eDonkey/Overnet-Leitungen). Es handelt sich hierbei um Server, welche dabei helfen, ein beschleunigtes „schwimmendes“ Herunterladen von einzelnen Teildatensegmenten zwischen Computern zu koordinieren.

Trotzdem nutzen neuere Netzwerke die Peer-to-Peer-Struktur für so ziemlich jeden Zweck bzw. jede Aufgabe. Aus diesem Grund werden sie auch „echte P2P-Netzwerke“ genannt. Darüber hinaus haben echte P2P-Netzwerke das unverwechselbare Merkmal, dass sich die gesamte Übermittlungs- oder Kommunikationsfähigkeit eines gewöhnlichen Nutzers mit der Anzahl der Nutzer/Netzknoten erhöht. Im Gegensatz zur verringernden Natur zentralisierter Systeme wird diese Tatsache durch die Technologie des Segment-Downloads unterstützt.

Ein weiteres wesentliches Feature der zweiten Generation von P2P-Netzwerken sind Multiprotokoll-Clients, welche in der Lage sind, innerhalb mehrerer Netzwerke (Protokolle) nach Daten zu suchen und diese herunterzuladen – manchmal sogar gleichzeitig. Hierzu gehören zB MLDonkey, KCeasy und Shareaza. Darüber hinaus sind sogenannte „Overlay-Protokolle“ ein integraler Bestandteil, welche eine Art „Supernetzwerk“ innerhalb eines bestimmten Netzwerks (Overnet) bilden.

Mit dem Aufkommen der dritten Generation von Netzwerken und Clients einher ging die Einführung bzw. die Verbesserung der Verschlüsselungselemente (Verschleierung des Datenverkehrs, welcher zum BitTorrent-Netzwerk hinzugefügt wurde), Anonymität oder Pseudo-Anonymität, sprich das verheimlichen der IP-Adressen von Computern/Netzknoten (Verschlüsselung des beidseitigen Routings oder Verknüpfens). Darüber hinaus versucht sie, eine größere Dezentralisierung zu erreichen, als das heute der Fall ist (Freenet, GNUnet). Tatsächlich kann man auf einige dieser Netzwerke nicht ohne die Zustimmung von anderen Nutzern zugreifen (Netzwerke wie Freund-zu-Freund, zB ANts P2P, WASTE, MUTE). Andere wiederum haben beinahe die Merkmale eines Virtual Private Network (VPN), zB I2P, welches das private Ausführen aller Internetaktivitäten erlaubt. Manchmal bieten solche Netzwerke nicht bloß Filesharing-Dienste an, sondern auch einen geschützten Bereich für die Kommunikation und Veröffentlichung von Dokumenten, ohne dass diese durch Zensur beeinträchtigt werden. Somit werden sie dezentralisiert und von einer privaten Groupware geschützt. Auf der anderen Seite sind die größten Nachteile dieser Systeme der geringere Nutzungskomfort sowie deren geringe Geschwindigkeit.

Die oben angesprochenen Internet-Radios und TV-Übertragungen (Internet-Streaming) des Typs Peer-to-Peer gehören manchmal zu den P2P-Anwendungen der vierten Generation (TVUPlayer, PPLive, PeerCast, PPStream). Ein bestimmter Teil von P2P-TV-Systemen basiert auf dem BitTorrent-Protokoll oder etwas ähnlichem (in diesem Fall geht es jedoch um Fernsehen „auf Abruf“, kein Live-Streaming). Gleichzeitig nutzen die größten davon ihre eigenen, unterschiedlichen Systeme. Alles in allem werden dutzende, wenn nicht gar hunderte von TV-Kanälen (oft Sport) auf diesem Wege übertragen – und zwar mit hoher Effizienz (vorausgesetzt, jeder empfangende Netzknoten kann zugleich auch ein rücküber-setzender Transmitter für andere Netzknoten sein.)

11.2. Filehosting

Dann gibt es da noch das Filehosting (sowohl frei als auch kommerziell) auf Web-Servern, einen im Wesentlichen ziemlich konservativen und technisch alten Dienst, der in Anbetracht der heutigen Verbindungsgeschwindigkeit jedoch sehr effektiv ist. In diesem Bereich gibt es über 100 wichtige ausländische Server, darunter auch so um die 10 tschechische. Die Voraussetzungen und Systeme für ihre Nutzung variieren je nach Server im Hinblick auf das Up- und Downloaden. Sie haben jedoch oft zwei verschiedene Download-Modi, sprich kostenlose Downloads können entweder nach Volumen oder Zeit eingeschränkt sein (finanziert durch Werbung und begrenzt durch OCR/Captcha-Systeme, temporäre Leitungen und Zeitintervalle) und "Bonus-Downloads", welche gegen Bezahlung einer kleinen Gebühr kaum bzw. uneingeschränkt zur Verfügung stehen. Eine begrenzte Liste dieser Server, ohne die dazugehörigen Domain-Endungen, welche sich mit etwas Recherche selbst weiter fortsetzen lässt, ist nachfolgend zu finden:

Im Ausland:
Rapidshare, depositfiles, filefactory, megaupload, mediafire, sendspace, uploading, zshare, ifolder, hotfile, icefile, letitbit, filefront, ifile, easy-share.

In Tschechien: Edisk, uloz.to, czshare, leteckaposta, quickshare, bagruj, nahraj.
In diesem Bereich gibt es ein paar Programme, welche bis zu einem gewissen Grad das Downloaden von diesen Servern automatisieren und somit erleichtern können. Dazu zählen zB der Universal Share Downloader (USD) oder RapGet. Andere wichtige Links sind:

- www.filesharing.eu Filesharing über P2P-Netzwerke
- www.slyck.com Nachrichtenplattform
- www.zeropaid.com Nachrichtenplattform
- www.filesharingz.com Nachrichten
- www.p2pnet.net Nachrichten
- www.p2pforums.com Diskussions- und Nachrichtenplattform
- www.infoanarchy.org Dezentralisiertes P2P-Wikiportal
- www.openp2p.com O´Reillys Website mit Fokus auf den P2P-Bereich
- www.planetpeer.de Plattform für anonyme Netzwerke, nicht nur für Filesharing (MUTE, I2P, Freenet etc.)
- www.fileshareworld.com Wegweiser für Austauschsysteme und P2P-Clients
- www.ftc.gov/bcp/workshops/filesharing Meinungen der US-Handelskommission über Filesharing
- http://cs.wikipedia.org/wiki/Peer-to-peer Tschechisches Wikipedia-Passwort
- http://p2ptv.yourglobaltv.com/, http://www.tvavailable.com/P2P_TV/ Überblick über die häufigsen P2P-TV-Clients
- http://en.wikipedia.org/wiki/P2PTV Augenöffnender Artikel über P2P-TV
- http://www.yourglobaltv.com/p2pchannels/ Hauptsportkanäle von P2P-TV
- http://en.wikipedia.org/wiki/File_hosting_service Allgemeines über Hosting-Server

- http://www.dimonius.ru/dusd.php automatischer Downloader Universal Share Downloader (USD)
- http://www.rapget.com/en/ RapGet ähnlich dem oben genannten USD.

12. ANONYMITÄT IM INTERNET

Die Anonymität im Internet war in letzter ein heiß diskutiertes Thema, sogar in den Regierungen hoch entwickelter Länder. Anonymität war schon immer ein wichtiger Faktor und ist es auch heute noch. Nichtsdestotrotz ist es aufgrund des Aufkommens neuer Technologien und ihres damit einhergehenden Siegeszugs in der Gesellschaft notwendig geworden, sich intensiver damit auseinanderzusetzen als bisher. Auf der anderen Seite haben einzelne Länder bereits erste Schritte eingeleitet, um das Internet einer stärkeren Kontrolle zu unterziehen. Nutzer sollen dadurch besser identifizierbar sein, womit die Sicherheit erhöht werden soll (dies zielt hauptsächlich auf die Bekämpfung von Terrorismus, Kinderpornografie, Drogenhandel und Geldwäsche ab). Gleichwohl versuchen Länder jedoch auch, die Privatsphäre und sensible persönliche Daten von Internetnutzern zu schützen, was von der EU mit der Durchsetzung eines sogenannten „Cookie-Gesetzes" unterstützt wurde.

Um die soziale Anonymität zu gewährleisten, müssen alle sieben Dimensionen von personenbezogenen Daten ausgeklammert werden:

- Vollständiger Name
- Wohnort
- Pseudonym, welches mit dem echten Namen oder dem Wohnort in Verbindung steht
- Pseudonym, welches auf andere persönliche Informationen schließen lässt
- Offenlegen von Verhaltensmustern
- Mitgliedschaft in einer bestimmten sozialen Gruppe
- Informationen, Objekte oder Fähigkeiten, welche auf persönliche Eigenschaften schließen lassen.

Die Gründe für die Wahrung der Anonymität bleiben in beiden Welten – sowohl der realen als auch der virtuellen – gleich: Das Vermeiden von Konsequenzen, die sich aus dem eigenen Verhalten ergeben (Furcht vor Repressionen, Missverständnissen usw.)

Identifizierungstechnologien

Moderne Technologien bieten eine Reihe von Wegen und Methoden zur Identifizierung von Individuen an.

IP-Adresse

Diese bezieht sich im Wesentlichen auf die eindeutige Adresse jedes Geräts, welches mit dem Netzwerk verbunden ist. Eine IP-Adresse kann zB Informationen über den geografischen Standort preisgeben.

Geolokalisierung

In letzter Zeit ist die Nutzung von Technologien, welche in der Lage sind, den Standort von Personen auf den Meter genau zu ermitteln, stark erhöht. Beispiele hierfür sind:

- Einschränkungsbasierte Geolokalisierung: Diese setzt auf das aktive Messen der Distanz über eine Antwort.

- GPS läuft hauptsächlich auf Mobiltelefonen.

- Eine Inhaltsanalyse von Web-Postings (Sozialen Netzwerken): Dies bezieht sich auf eine Methode der Lokalisierung von Nutzern auf Grundlage der Analyse von öffentlich verfügbaren Postings, zB nach der Stadt, dem Land oder dem Wetter, welche bzw. welches im Inhalt des Postings zu finden ist. Darüber hinaus lässt die Aktivität eines Nutzers zu einer bestimmten Zeit einen Schluss auf die Zeitzone zu, in der er sich befindet.

Cookies

Cookies dienen als ständiger Identifikator zwischen einem Client und einem Server. Durch ihr Eindringen in die Privatsphäre der Nutzer wird mit Cookies innerhalb der Europäischen Union jedoch sehr kritisch umgegangen.

PRISM

PRISM bezieht sich auf ein staatliches Projekt des US-amerikanischen Sicherheitsdienstes NSA. Dieses Projekt hat uneingeschränkten Zugriff auf Daten von Google, Microsoft, Yahoo und viele andere Dienste, welche mit Blick auf die oben genannten Unternehmen 98% aller Daten erzeugen. Trotzdem leugnen besagte Unternehmen, dass sie unbeschränkten Zugang zu all diesen Daten haben.

12.1. Technologien zum Schutz der Privatsphäre

Tor bezeichnet ein Projekt, welches auf dem Onion Routing-Konzept basiert und damit die Anonymität der Nutzer sicherstellt, während diese im Internet surfen. Das Programm ist darauf ausgelegt, die personenbezogenen Daten der Nutzer, die Privatsphäre sowie die Möglichkeit auf den geheimen Abschluss von Geschäften zu schützen, indem es die Nutzer davor bewahrt, dass ihre Aktivitäten im Internet nachverfolgt werden. Eben diese Software lässt sich jedoch auch für illegale Aktivitäten missbrauchen, da die Verwendung dieser Technologie das Ausforschen von Kriminellen erschwert.

Orbot bezeichnet die Tor-Version für Mobiltelefone mit dem Betriebssystem Android.

Freenet-Projekt wird als eine vollkommen sichere, anonyme und dezentralisierte Plattform zum Teilen von Daten betrachtet, deren Zweck darin besteht, die Zensur auszuhebeln. Jeder Nutzer stellt einen Teil seiner lokalen Festplatte zur Verfügung, auf welchen das gesamte Netzwerk zugreifen kann. Darauf können verschlüsselte Daten von anderen Nutzern gespeichert werden. Dadurch wird kein eigener privater Server benötigt.

Das Internet umfasst ein ausgedehntes und komplexes Netzwerk von Kommunikationskanälen, über welche Daten fließen. Jedes **Datenpaket** (in der Folge nur noch "Paket" genannt) enthält – abgesehen vom Inhalt selbst, welcher irgendwo hingeschickt werden soll – bestimmte Erkennungsmerkmale, welche von besonderem Interesse für neugierige Behörden und Unternehmen sind. Dazu gehören **Google, Microsoft, Facebook, Twitter** usw.

In der Tat nutzen diese Firmen **Erkennungsmerkmale** von Nutzerdaten, um herauszufinden, welche Webseiten für sie von Interesse sind, wie oft sie diese besuchen und auch, von wo aus sie darauf zugreifen. In der Folge werden diese wertvollen Informationen ausgewertet, um zielgerichtete Werbeanzeigen schalten zu können. Seit dem Aufkommen sozialer Netzwerke geht diese Spionage noch deutlich weiter.

Die großen Behörden und Unternehmen, welche auch "Big Brother" genannt werden, können die Online-Aktivitäten von Nutzern erfolgreich mit jenen ihrer Freunde **kombinieren** und somit eine genaue Karte der Internetnutzer zeichnen. Dieser **freiwillige Verzicht auf die Privatsphäre** ist der Preis für die kostenlose Bereitstellung von Diensten. Auf der anderen Seite, um nicht nur die Nachteile von diesen Serviceanbietern aufzuzeigen, ist es notwendig darauf hinzuweisen, dass ihre Dienste qualitativ sehr hochwertig und durchdacht sind, auch wenn dies auf den ersten Blick nicht so scheinen mag.

12.2. Grundprinzipien zur Wahrung der Anonymität

Wie bereits gesagt wurde, verfolgt das Internet hauptsächlich, woher unsere Daten kommen und ob sie zu uns gehören. Daher besteht die Hauptaufgabe darin, diese **Daten zu verschleiern**. Zu diesem Zweck sollte man auf VPNs (Virtual Private Networks), Proxy-Server oder spezielle Internetbrowser setzen. Die Vor- und Nachteile der einzelnen Lösungen werden nachfolgend vorgestellt.

Verbindung via VPN

Virtuelle private Netzwerke werden vor allem in Unternehmen verwendet, wo sie es mehreren Computern ermöglichen, auf Netzwerkspeicher, Drucker oder andere Server zuzugreifen. Gleichzeitig stellen sie eine Kommunikation zum frei zugänglichen Internet her. Des Weiteren werden Datenpakete mit der IP-Adresse eines VPN-Servers markiert, nicht mit jener des Computers, damit Big Brother sie diesem nicht zuordnen kann.

Loggt man sich in ein VPN ein, welches sich in einem anderen Land befindet, kann der physische Standort nicht herausgefunden werden. Darüber hinaus verschlüsselt ein VPN-Server die Kommunikation, damit abgesehen vom Ende-zu-Ende-Server niemand in der Lage ist, die Daten auszulesen.

Es gibt viele VPNs aus den verschiedensten Orten der Welt, welche für das anonyme Surfen im Internet bestimmt sind. Leider sind sie verpflichtet, die IP-Adresse von Nutzern offenzu-legen, wenn sie von einem Gericht dazu aufgefordert werden: Anderenfalls würden sie verboten werden. Deshalb kann man sich nicht darauf verlassen, dass niemand dazu in der Lage ist, die IP-Adresse eines Nutzers herauszufinden, nur weil er einen VPN-Dienst nutzt.

Verbindung via Proxy-Server

Ebenso wie ein VPN-Server stellt auch ein Proxy-Server die Kommunikation zwischen einem PC und dem Internet her. In diesem Fall wird das Internet Nutzerdaten so betrachten, als gehörten sie zum Proxy-Server. Anders als bei einem VPN werden die Daten jedoch nicht verschlüsselt. Da Proxy-Server eine einfachere Lösung als VPNs darstellen, ist es auch möglich, Proxy-Server für öffentlich zugängliche Online-Schnittstellen zu verwenden.

In der Tat lassen sie sich leicht einsetzen, wenn es um eine kurzfristige Anwendung geht. Man muss nur die richtige Adresse in ihre Adresszeile eintragen. Dadurch stellt der Proxy-Server eine Kommunikation mit dem bestimmten Web her.

Gleichwohl muss man beachten, dass alle Nutzerdaten über den Proxy-Server laufen, sprich im Falle eines unzuverlässigen Proxy-Servers können Daten missbraucht werden. Aus diesem Grund wird davon abgeraten, Proxy-Server für den Besuch geschützter Webseiten (https) zu benutzen.

Spezielle Web-Browser und Suchmaschinen

Anonyme Web-Browser konzentrieren sich auf Layman's Erwartungen an seinen üblichen Browser, wenn der Anonymitätsmodus eingeschaltet ist. Dieser Modus versucht nicht um jeden Preis, die Internetaktivitäten eines Nutzers vor Big Brother zu schützen – sondern nur vor anderen Nutzern desselben Computers. Somit wird der gesamte Internetverkehr wie üblich nachverfolgt.

Im Gegensatz dazu sind anonyme Web-Browser so programmiert, dass sie Big Brother daran hinder, Nutzerdaten auszuspähen. Auch wenn diese Lösung nicht außergewöhnlich effektiv ist, so ist sie zumindest einfach und schnell. Darüber hinaus ist es sehr angenehm, einen Browser mit einer anonymen Internetsuchmaschine statt Google, Yahoo oder Bing zu verwenden, da dieser Browser keine Informationen darüber speichert, wonach der Nutzer gesucht hat.

Onion Routing – Tor

Tor ist ein Web-Browser und auch ein Server-Netzwerk. Es wird oft als Internet im Internet bezeichnet. Es arbeitet nach dem Prinzip des Onion Routings, demzufolge jedes Paket in Schichten verschlüsselt ist – wie eine Zwiebel – und jeder Server nur dazu in der Lage ist, eine Schicht zu dechiffrieren.

Dadurch durchläuft jedes Paket eine bestimmte Anzahl von Servern (zumindest drei), bevor es sein Ziel erreicht. Nichtsdestotrotz kennt jeder Tor-Server nur die Adressen des Ankunfts- und Ausgangsservers, nicht jedoch die gesamte Kaskade.

Deshalb ist es fast unmöglich, ein Paket bis zu seiner ursprünglichen IP-Adresse zurückzuverfolgen. Tor hat auch dadurch einen zweifelhaften Ruf erworben, dass es einen Zugang zum Darknet erlaubt, in welchem allerlei illegale Aktivitäten stattfinden. Der größte Nachteil beim Einsatz eines Tor-Browsers ist dessen geringe Geschwindigkeit, da die darüber transferierten Daten buchstäblich in und quer durch die gesamte Welt reisen.

12.3. TOR: Total anonymes Internet

Digitaler Fußabdruck

Jeder Nutzer des weltumspannenden Netzwerks hinterlässt Spuren seiner Aktivitäten. Dieses Phänomen wird seit den 1980ern als „digitaler Fußabdruck“ bezeichnet. Zu einem gewissen Grad hängt die Intensität des Fußabdrucks – zumindest in der ersten Phase – vom Nutzer ab: Dies gilt vor allem für die Browser-Einstellungen oder die Installation des Proxy-Servers, welcher die Kommunikation zwischen dem internen Netzwerk und dem Internet bereitstellt und somit eine Reihe von Sicherheitseinstellung ermöglicht. Alles in allem garantiert er keine vollständige Anonymität, gewährleistet jedoch den adäquaten Schutz der Privatsphäre für die übliche Nutzung des Internets.

Ein effektiverer Schutz

Zu Beginn des Jahrhunderts wurde mit Argusaugen auf die Anonymität im Internet geachtet. Ein paar Projekte wurden ins Leben gerufen, um Nutzer mit einem geeigneten Schutz ihrer Privatsphäre auszustatten. Besondere Aufmerksamkeit kam dem Projekt des Tor-Netzwerks zu (Onion-Routing), da es von der US-amerikanischen Regierungsbehörde Naval Research Laboratory gegründet und finanziert wurde. Zunächst diente es zum Schutz der Regierungs-kommunikation in den USA. Eine weitere finanzielle Förderung erhielt Tor von der gemein-nützigen Organisation Electronic Frontier Foundation, welche sich mit dem Schutz von Rechten in der digitalen Sphäre beschäftigt.

Knoten neben dem Knoten

Wie funktioniert ein vollständig anonymes Netzwerk? Das Sicherheitsprinzip basiert auf einer großen Anzahl an Knoten, welche der Datenstrom passiert. Die gesamte Kommunikation wird asymmetrisch verschlüsselt und Server teilen öffentliche Schlüssel und tauschen erzeugte dynamische Schlüssel aus um untereinander Datenstrings zu übermitteln. Jeder Knoten ist völlig autonom und zieht die Information darüber, wohin der String zu senden ist, nur aus dem Nachrichtenkopf. Damit endet sein Wissen über den Datenfluss beim nächsten Knoten. Um es einfacher auszudrücken: Der Server weiß, an wen eine bestimmte Information geschickt werden soll und an wen die Antwort zurückgehen soll. Andere Aktivitäten übersteigen jedoch seine Fähigkeiten. Je mehr Knoten eingebunden sind, desto höher ist die Anonymität. Der Netzwerknutzer selbst wählt einen geeigneten Pfad, über welchen die Daten geschickt werden sollen.

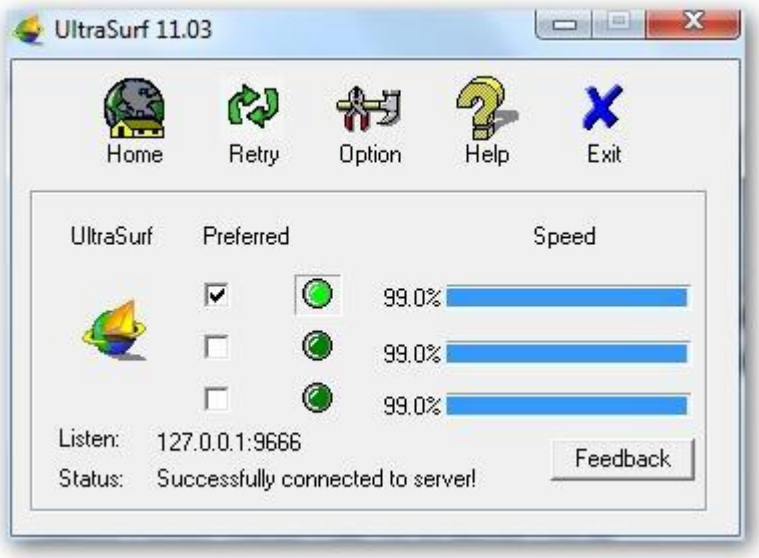
Falsche Fußabdrücke

Die Komplexität des Datentransfers über anonyme Netzwerke scheint auf den ersten Blick sehr zufriedenstellend zu sein: Tor geht jedoch noch weiter. So können seine Server Pakete zB in einer anderen Reihenfolge verschicken, als sie empfangen werden. Ebenso können falsche Pakete können zwischen den übermittelten Datenstrings eingeführt werden, welche eine mögliche Nachverfolgung des Datenstroms vom tatsächlichen Pfad umlenken. Der Hauptnachteil des Tor-Netzwerks ist dessen lange Reaktionszeit.

Darüber hinaus gibt es Situationen, in welchen ein Nutzer, um seine Privatsphäre zu schützen oder auf einige Dienste zuzugreifen, seine IP-Adresse ändern muss. Dies ist trotzdem eine heikle Operation: Viele Dienste bieten eine Lösung über ein VPN und ihren eigenen Client mit Extra-Funktionen an, einen Zugriff auf ihre eigenen Server, wodurch die Kommunikation so umgeleitet wird, dass der Nutzer entweder anonym oder verschlüsselt im Internet surfen kann.

UltraSurf

UltraSurf ist ein minimalistisches Programm, welches selbst absoluten Anfängern anonymes Surfen im Internet erlaubt. Erreicht wird dies vor allem durch einfache Einstellungen, Bedienung, günstigen Betrieb und freie Verfügbarkeit. Das Programm im kleinen Fenster bietet eine Verbindung zu drei verschiedenen Servern an.



Die erfolgreiche Änderung der IP-Adresse wird von einem Icon in Form eines Vorhängeschlosses in der Toolbar angezeigt. Darüber hinaus ist es möglich, die Bedienungs-elemente mithilfe von Tastenkombinationen ein- bzw. auszuschalten, den Browser zu starten, automatisch Cookies und Verlauf zu löschen sowie den Proxy-Server einzurichten. Um auf US-amerikanische Server und Dienste zuzugreifen, welche eine locale IP-Adresse benötigen, nutzt UltraSurf den “freekarol”-Reader, womit es zu den besten kostenlosen Anwendungen gehört.

proXPN

Dieser VPN-Client ist sehr beliebt und wird oft verwendet, da er eine gute Leistung, qualitativ hochwertige Dienste, die Wahl zwischen einer US-amerikanischen, britischen, holländischen und singapurischen IP-Adresse, Verschlüsselung, unbegrenzten Datentransfer, zeitlich begrenzte Informationsspeicherung über die Verbindung (zwei Wochen) und eine Reihe weiterer Features anbietet. Das Programm umfasst in der kostenlosen Version die obengenannten Dienste, weitere Features gibt es gegen Gebühr.

TunnelBear VPN

Benutzer bezeichnen den Dienst TunnelBear und seine VPN-Anwendung als schön, sehr einfach und nutzerfreundlich. Darüber hinaus ist es möglich, eine kostenlose Version zu verwenden, welche es erlaubt, 500 MB Datenvolumen pro Monat kostenlos durch den „Tunnel“ zu schleusen. Darüber hinaus gibt es 1 GB extra, wenn man ihn auf Twitter empfiehlt. Gegen eine Gebühr von fünf US-Dollar pro Monat bekommt man die Möglichkeit, auf die unlimitierte Version zuzugreifen.

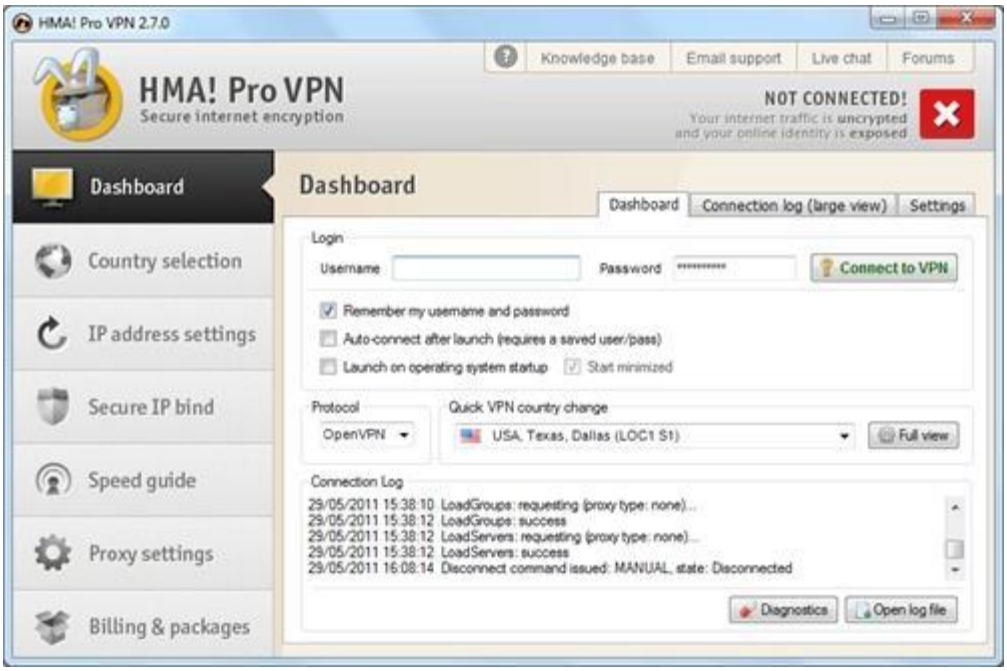
CyberGhost VPN

Ein weiteres empfohlenes Tool ist CyberGhost, welches eine verschlüsselte Verbindung (1024 Bit SSL 128 Bit AES-Passwort) zu einem VPN über einen Software-Client voraussetzt, über welchen die weitere Kommunikation mit dem Internet geführt wird. Das Programm ist leicht zu bedienen und bereits mit wenigen Klicks ist eine Verbindung hergestellt.

Das Server-Netzwerk von CyberGhost ist beständig und effizient. Darüber hinaus ist der Geschwindigkeitsverlust im Vergleich zu anderen Lösungen äußerst gering. Das Programm bzw. der Dienst können kostenlos genutzt werden, wenn auch nur mit funktionellen Einschränkungen (1 GB Datenvolumen pro Monat mit einer Geschwindigkeit von 2 MBit/s usw.). Darüber hinaus bieten die Hersteller verschiedene bezahlte und nach Effizienz gestaffelte Versionen an. CyberGhost wurde von Suslikus empfohlen.

Hide My Ass

Hide My Ass ist ein weltbekanntes VPN, welches eine breite Nutzerbasis hat und über ein breites Spektrum an Diensten und Servern verfügt. Hide My Ass hat fast 40.000 IP-Adressen in 53 verschiedenen Ländern im Angebot, hinter welchen man sich verstecken kann. In der Tat können kostenlose Lösungen nicht mit so einer großen Zahl an IP-Adressen mithalten, dafür fallen jedoch auch mehr als 11 US-Dollar pro Monat an Nutzungsgebühr an. Wenn man sich für ein langfristiges Abonnement entscheidet, reduziert sich der Preis jedoch auf sechseinhalb US-Dollar.



13. ANGRIFF UND VERTEIDIGUNG IM INTERNET

13.1. Angriff und Verteidigung des PCs

13.1.1. Angriff

Virus

Der Name leitet sich aus der Analogie zum Virus biologischen Ursprungs ab. Er kann sich selbst reproduzieren – vorausgesetzt, es gibt einen funktionstüchtigen Wirt, mit welchem er verbunden ist. Ein Wirt kann aus ausführbaren Dateien, Systemplattenbereichen oder Dateien bestehen, welche nicht direkt ausgeführt werden können, aber über den Umweg einer bestimmten Anwendung (Microsoft Word-Dokumente, Visual Basic Scripts usw.). Wird der Wirt gestartet, wird zeitgleich der Virus-Code dechiffriert. Zu diesem Zeitpunkt versucht der Virus für gewöhnlich, eine weitere Selbst-Reproduktion sicherzustellen – und zwar durch das Herstellen einer Verbindung zu anderen geeigneten lauffähigen Wirten.

Trojaner

Anders als ein Virus kann dieser Schadcode sich nicht selbst reproduzieren und Dateien infizieren. Ein Trojaner scheint meist eine ausführbare EXE-Datei zu sein, welche nichts (Nützliches) enthält, sondern nur den Trojaner. Sobald er aktiviert wurde, gibt es – da der Trojaner sich nicht mit einem Wirt verbindet – nur eine Möglichkeit der Desinfektion: Die Löschung der infizierten Datei. Eine ältere Definition besagt, dass obwohl ein Trojaner nützlich zu sein scheint, er in Wahrheit ziemlich schädlich ist. Vor langer Zeit tauchte ein Trojaner auf, der wie ein Virusscanner von McAfee aussah, jedoch nichts anderes Tat, als Daten auf der Festplatte zu entfernen. Aktuell stößt man mitunter auf folgende Arten:

- passwortstehlender Trojaner (PWS)
- zerstörerischer Trojaner
- Backdoor-Trojaner
- Proxy-Trojaner

Wurm

Ursprünglich bezog sich der Begriff „Wurm“ auf „Morris Wurm“, welcher 1989 einen beachtlichen Teil des damaligen Netzwerks befiehl, welches sich später zum Internet entwickelte. Dieser und andere Würmer (die aktuellsten sind Code Red, SQL Slammer, Lovsan/Blaster, Sasser usw.) operieren auf einer niedrigeren Netzwerkebene als gewöhnliche Viren. Sie verbreiten sich nicht in Form von befallenen Dateien, sondern als Netzwerkpa-

Diese Pakete werden von einem erfolgreich infizierten System an andere Internetsysteme gesendet (entweder zufällig oder über einen bestimmten Schlüssel). Erreicht solch ein Paket ein System mit einer bestimmten Sicherheitslücke, kann dieses infiziert werden, wodurch in der Folge weitere „Wurmpakete“ produziert werden können. Folglich verbreiten sich Würmer, indem sie bestimmte Sicherheitslücken des Betriebs-systems ausnutzen. Der Erfolg von Würmern hängt von der Verbreitung der Software ab, welche ausnutzbare Sicherheitslücken hat. Wie sich aus den oben genannten Charakteristika vielleicht ableiten lässt, können Würmer nicht von einer herkömmlichen Antivirensoftware entdeckt werden. Daraus folgt, dass als Nebeneffekt eine ernsthafte Netzwerkinfektion auftreten kann, welche auch ein Unternehmens-LAN betreffen kann. Der Begriff „Wurm“ wird oft mit einer Infiltrationsart assoziiert, welche per E-Mail verbreitet wird. In diesem Fall überschneiden sich die Begriffe „Wurm“ und „Virus“.

Spyware

Der Ausdruck Spyware bezieht sich auf ein Programm, welches das Internet nutzt, um ohne das Wissen eines Nutzers Daten von einem Computer zu verschicken. Anders als ein Backdoor-Trojaner stiehlt diese Schadsoftware nur statistische Daten wie eine Aufstellung der besuchten Webseiten oder installierten Programme. Dies wird gemacht, um die Bedürfnisse und Interessen von Nutzern herauszufinden und diese Informationen für gezielte Werbung zu nutzen. Es gibt jedoch keine Garantie, dass sich diese Informationen oder Technologie nicht auch missbrauchen lassen. Deshalb gibt es eine Menge von Nutzern, welche über die bloße Existenz und Legalität von Spyware erzürnt sind. Dazu mag sicher auch kommen, dass Spyware häufig mit ausdrücklicher Zustimmung ihrer Verfasser mit einer großen Zahl von Shareware-Programmen verbreitet wird.

Adware

Diese bezieht sich auf ein Produkt, welche durch Werbung am PC die Arbeit mit diesem erschwert. Die typischen Symptome sind Pop-Up-Werbefenster beim Surfen und aufdringliche Webseiten (zB Startseiten im Internet Explorer), welche für den Nutzer uninteressant sind. Oft ist eine „EULA“, was Endbenutzer-Lizenzvertrag bedeutet, Teil dieser Adware, aufgrund welcher der Nutzer in vielen Fällen der Installation zustimmen muss. Adware kann Teil eines bestimmten Produkts (zB BSPlayer) sein. Im Gegenzug dafür, dass man die ständige Werbeeinblendung akzeptiert, bekommt man als Belohnung eine größere Zahl nützlicher Funktionen, welche eine gemeinhin kostenfreie Version (werbefrei) nicht bietet.

Dialler

Ein Dialler ist ein Program, welches die Art des Internetzugangs via Modem verändert. Anstelle der üblichen Telefonnummer für die die Internetverbindung leitet das Wählprogramm das Modem auf eine Mehrwertnummer um, zB 60 Kronen/Minute. Man muss jedoch anmerken, dass diese Dialler nur in Zeiten der analogen Telefonleitungen (Ein-Wähl-

Verbindungen) effektiv waren und ADSL oder andere moderne Technologien nicht davon betroffen sind.

Phishing

Dieser Begriff bezieht sich auf betrügerische E-Mails, welche so aussehen, als ob sie von einer größeren Organisation (zB einer Bank) kommen würden und welche an einen großen Verteiler von Adressen verschickt werden. Diese E-Mails setzen stark auf „Sozialtechnik“, sprich dem Empfänger wird suggeriert, dass er sensible Daten in ein ausführliches Formular eintragen muss, da ansonsten sein Bankkonto (im Falle einer Bank) gesperrt wird oder er im Falle einer Weigerung irgendwelche anderen Nachteile zu erwarten hat. Solche E-Mails enthalten in der Regel einen Link zu einer Website mit diesem Formular, welche vorgaukelt, sich auf dem Server besagter Organisation zu befinden. In Wahrheit jedoch wird der Nutzer an einen externen Server weitergeleitet, welcher im Design der tatsächlichen Organisationswebsite gehalten ist. Daher kann der Nutzer, welcher darauf herein-gefallen ist, keinen Unterschied feststellen und füllt die leeren Eingabefelder wie aufgefordert mit vertraulichen Informationen, Kontonummern, Passwörtern für das InternetBanking, PIN-Code für die Bezahlung usw aus. Die auf diesem Wege erhaltene Information kann von Betrügern leicht missbraucht werden.

13.1.2. Schutz

Leider wird dem Begriff “Prävention” von PC-Nutzern nur wenig Bedeutung beigemessen. Nichtsdestotrotz ist es notwendig zu begreifen, dass das bloße Installieren von Antivirensoftware (auch wenn diese regelmäßig aktualisiert und korrekt konfiguriert ist) eine unzureichende Vorkehrungsmaßnahme ist. Regelmäßiges Updaten von zumindest all jenen Produkten, welche mit einem Computernetzwerk des Internets in Verbindung stehen, sind von zentraler Bedeutung. Kurz gesagt fällt darunter:

- das Zulassen regelmäßiger Updates des Betriebssystems Windows und seiner integralen Bestandteile (Start/Steuerkonsole/Automatische Updates)

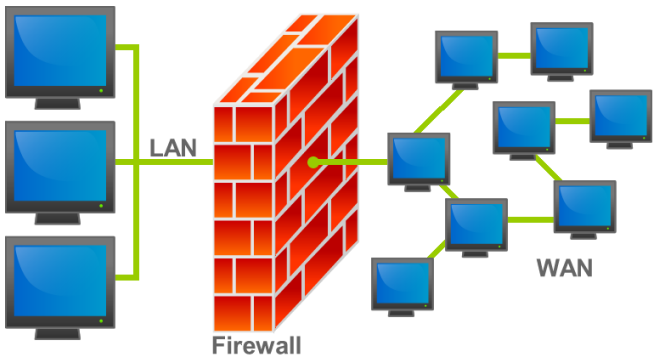
- das regelmäßige Updaten anderer häufig verwendeter Produkte, welche vom Internet aus missbraucht werden könnten (Mozilla, Firefox, ICQ, DC++). Alternativ kann es ausreichen, regelmäßige Auto-Updates zu aktivieren. Klarerweise betrifft das auch zahlreiche „Plugins“ von bestimmten Browsern (Java, Shockwave, Flash Player)

Antivirensoftware

Antivirensoftware sollte ein integraler Bestandteil jedes PCs sein. In den meisten Fällen ist ein großer Teil dieser Antivirensoftware auch ein Schutz vor Spyware. In diesem Zusammenhang ist es notwendig, Antivirensoftware und Anti-Spyware regelmäßig automatisch updaten zu lassen. Angesichts der rasanten Geschwindigkeit, mit welcher sich Gefahren (hauptsächlich per E-Mail) verbreiten, ist ein Update jede halbe Stunde keine Utopie. Alles in allem lässt sich über Updates dieser Software sagen: Je öfter, desto besser. Ebenso wichtig ist es, stets Moduldurchläufe durchführen zu lassen, um Dateien zu finden, welche von Hackern oder Anwendungen manipuliert werden (öffnen/speichern/ausführen usw.) Solch ein Modul bezeichnet man gemeinhin als „Bürger-schild" oder – etwas technischer – „On-Access Scanner". Man muss sich auch bewusst sein, das dieses Modul der wichtigste Bestandteil einer Antivirensoftware ist. Obwohl derzeit in den meisten Fällen ein Modul angeboten wird, welches direkt heruntergeladene oder versendete Post inspiziert, mag es in Zukunft an Bedeutung verlieren, da eine mögliche Infektion ohnehin von dem On-Access-Sanner verhindert wird (mit ein paar Ausnahmen, welche Fehler in einem Programm ausnutzen). Obwohl ein Virus nicht identifiziert wird, bevor er im Posteingang landet, würde er in dem Moment erkannt werden, in dem ein Nutzer versucht, ihn zu öffnen, sprich den infizierten E-Mail-Anhang zu öffnen.

Firewall

Eine Firewall, zumeist eine persönliche Firewall, ist eine nützliche Ergänzung für all jene Nutzer, die auf das Internet zugreifen. Eine Firewall ist zu jenem Zeitpunkt nahezu unerlässlich, in dem sich ein Nutzer über seine IP-Adresse und seinen Computer mit dem Internet verbindet (ein Benutzer bekommt für gewöhnlich eine öffentliche IP-Adresse durch die Einwählverbindung oder eine Verbindung über das Internetkabel zugewiesen – Chello/UPC.) Ebenso wie Antivirensoftware muss eine Firewall sachgemäß verwendet werden. Daher sollte ein Nutzer in der Lage sein, zwischen einer legalen und einer illegalen Verbindung zu unterscheiden, sprich zu wissen, was erlaubt und was verboten gehört. Anderenfalls kann die Firewall ihren Zweck nicht erfüllen, unabhängig davon, ob man die in Windows integrierte Firewall oder eine andere, kostenpflichtige Firewall verwendet.



13.2. Gefährliches Netzwerk: Angriffe abwehren

Leider lauern in Netzwerken zahlreiche Gefahren. Es gibt tausende Applikationen, welche sich theoretisch und praktisch für Angriffe missbrauchen lassen. Vor manchen dieser Gefahren kann man sich relative leicht schützen, zB durch Beachten geeigneter Sicherheitsmaßnahmen. Dazu gehören starke Passwörter und das regelmäßige Installieren aktueller Software-Updates. Es gibt jedoch auch Gefahren, vor welchen man nicht gefeit ist und die äußerst schwer zu entdecken sind. Auf eben diese wird im weiteren Verlauf des Kapitels eingegangen.

Diese betreffen hauptsächlich Angriffe, welche über das TCP/IP-Protokoll ausgeführt werden. Dieses Protokoll ist über 30 Jahre alt und man fand heraus, dass nicht alles korrekt entworfen und angelegt wurde. Auf der anderen Seite muss man auch die Bedingungen anschauen, unter welchen das TCP/IP Protokoll designt und ins Leben gerufen wurde. Es ist evident, dass zum Zeitpunkt seiner Entwicklung unmöglich vorherzusehen war, dass das weltumspannende Computernetzwerk innerhalb weniger Jahrzehnte hunderte Millionen Nutzer haben würde. Mit größtmöglicher Vorsicht und durch das Einhalten geeigneter Sicherheitsmaßnahmen lassen sich jedoch auch vor nachfolgend beschriebenen Gefahren schützen.

Überwachung des Netzwerkverkehrs

Die Überwachung des Netzwerkverkehrs wird gemeinhin als “Sniffing” bezeichnet. Im Grunde handelt es sich hierbei um eine Analyse des Netzwerkverkehrs. Nachfolgend werden die Prinzipien und Bedingungen vorgestellt, nach bzw. auf deren Grundlage ein Angriff passieren kann. Zunächst muss man festhalten, dass diese Art von Angriffen für gewöhnlich in LAN-Netzwerken durchgeführt wird. Eine weitere Voraussetzung ist, dass das Netzwerk keine geschaltete Verbindung nutzt (diese Bedingung kann vernachlässigt werden, wie nachfolgend erklärt wird). An dieser Stelle wird erklärt, wie die Kommunikation in einem LAN-Netzwerk funktioniert. Alle Daten, unabhängig davon, woher sie kommen bzw. wohin sie gehen, durchqueren ein Übertragungsmedium (Kabel) in Form eines Clusters, welcher als „Frame“ bezeichnet wird. Jeder Frame ist für eine bestimmte MAC-Adresse konzipiert, sprich eine Adresse jeder Netzwerkkarte. In den meisten Karten ist die Adresse unveränderlich und vom Hersteller zugewiesen. Darüber hinaus erhält jede Karte im gleichen Netzwerksegment alle Frames, welche das Übertragungsmedium durchqueren und findet heraus, ob diese für sie bestimmt sind. Falls ja, gibt die Karte den Frame an eine höhere Schicht zur Verarbeitung weiter, ansonsten wird er ignoriert. Gleichwohl kann sich eine einmalige Situation ergeben, in welcher ein Frame für alle MAC-Adressen gültig ist (Rundfunk).

Gehen wir nun davon aus, dass Sie von einem Computer mit Verbindung zu einem LAN-Netzwerk aus mit einem lokalen Mail-Server verbunden sind. Sie geben dort Ihren Benutzernamen und Ihr Passwort ein und laden Ihre Post ohne Probleme herunter. Dabei bemerken Sie jedoch nicht, dass der Kollege neben Ihnen oder jemand am anderen Ende

vielleicht ihr Passwort oder ihre Nachrichten liest. Dies ist jedoch durchaus möglich. Für den Kollegen ist dies ganz einfach: Es gibt schließlich Programme, welche selbst dann das Auslesen von Frames erlauben, wen diese für eine andere MAC-Adresse bestimmt sind. Solche Programme nennt man Sniffing-Tools. Man muss das Programm nur installieren und starten – der Rest wird vom Programm erledigt. Einen fähigen Programmierer stellt das Schreiben eines solchen Programms vor keine große Herausforderung. Das Programm versetzt die Netzwerkkarte in einen sogenannten "Promiskuitätsmodus", welcher es ihm ermöglicht, den gesamten Verkehr in einem bestimmten Netzwerksegment zu überwachen und zu analysieren. Es gibt einfache Sniffing-Tools, zB UNIX TCPDUMP, oder äußerst fortgeschrittene wie Hunt. Effektiv vor Hunt schützen kann man sich nur mit entsprechender Verschlüsselung. Solange der Verkehr verschlüsselt ist, sind die Daten für einen Hacker nutzlos, da er sie nicht lesen kann. Die vorteilhaftesten Alternativen sind SSH und SSL. Daher ist es günstig, aktuelle Dienste zu ersetzen, welche Textpasswörter verwenden. Nichtsdestotrotz ist es notwendig zu wissen, wer den Verkehr überwacht. Handelt es sich um jemanden aus dem lokalen Netzwerk, lassen sich dagegen schwer Schutzmaßnahmen ergreifen. Es gibt jedoch Programme, welche in der Lage sind, Netzwerkkarten zu finden, welche sich aktuell im Promiskuitätsmodus befinden.

Denkbar ist aber auch, dass ein Sniffing-Tool auf einem Computer innerhalb eines LAN-Netzwerks durch einen Eindringling von außen installiert wird. Wenn es ihm gelingt, so ein Netzwerk zu hacken, wird er das höchstwahrscheinlich machen, da es keinen einfacheren Weg gibt, an Informationen über zahlreiche Benutzernamen und Passwörter heranzukommen. Der wirkungsvollste Schutz ist, das Netzwerk abzusichern, sodass niemand es hacken und ein Sniffing-Tool installieren kann.

DNS

DNS (Domain Name Service) bezieht sich auf einen der wichtigsten Dienste, den man in einem Netzwerk finden kann. Er stellt sicher, dass Domainnamen in IP-Adressen überführt werden und umgekehrt. Darüber hinaus macht dieser Service täglich das Leben von Millionen Benutzern leichter. Jedes Objekt (Server, Router), welches Teil eines IP-basierten Netzwerks ist (Intranet, Internet), besitzt eine exklusive Identifikation. Diese Identifikation wird durch die IP-Adresse repräsentiert. Hierbei handelt es sich um eine Nummer mit folgendem Format: xxx.xxx.xxx.xxx, zB 192.168.1.1. Diese Nummer ist exklusiv und kann nicht von zwei Objekten geteilt werden, welche gleichzeitig mit dem Netzwerk verbunden sind. Diese eindeutige Kennung hat jedoch eine namentliche Alternative, zB http://www.firma.cz, und die Um- und Rückwandlung zwischen diesen zwei Identifikatoren wird durch DNS sichergestellt. Man kann festhalten, dass sich Adressen wie http://www.pcworld.cz oder http://www.google.com leichter merken lassen als ein "bizarrer Zahlenmix". Im weiteren Verlauf dieses Kapitels wird die DNS-Funktionsweise im Detail beschreiben. Zu diesem Zweck wird in den folgenden Absätzen auf den Missbrauch von DNS eingegangen.

DNS-Manipulation

Eine DNS-Manipulation ist eine ziemlich gefährliche Aktivität. Um sie auszuführen, ist es notwendig, ein paar Anforderungen zu erfüllen. Unabdingbar ist in diesem Zusammenhang, dass der Hacker den Netzwerkverkehr überwacht (siehe oben). Unter der Voraussetzung, dass er Zugriff auf das LAN hat, kann er ein Programm auf seinem Computer starten, welches alle DNS-Anfragen abfängt und versucht, diese im Sinne des Hackers zu beantworten. Folglich ist das Hauptziel, die DNS-Antworten zu unterwandern und den Gast auf ein anderes System umzuleiten. So kann ein Hacker zB einen Netzwerk-Server haben, bei welchem es sich um eine perfekte Kopie eines E-Mail-Webservers handelt, welcher auf den ersten Blick identisch zum Original ist. Der Hauptzweck dieser Handlung besteht darin, alle Nutzer eines Netzwerks direkt auf diesen Server umzuleiten. Gibt ein Nutzer http://www.webmail.something mit der tatsächlichen Adresse 192.168.1.1 in seinen Browser ein (diese Adresse ist eigentlich nicht verfügbar, da sie sich auf die Adresse eines privaten Adressblocks bezieht, welcher für Netzwerke verwendet wird, die nicht direkt mit dem Internet verbunden sind; sie wird nur zu Illustrationszwecken verwendet), versucht das Hackerprogramm, die DNS-Antwort zu unterwandern und antwortet dem Client damit, dass der Server http://www.webmail.something eine 192.1691.100-Adresse hat. Im Fall, dass diese Antwort vor der Antwort des tatsächlichen und originalen DNS-Servers im Nutzersystem einlangt, gewinnt der Hacker. Wie lassen sich solche Angriffe vermeiden? Das erste und grundlegende Prinzip ist es, den Hacker am Eindringen in das Netzwerk zu hindern. Gelingt im das nicht, kann er nichts machen. Wenn ein autorisierter Nutzer sich jedoch auf diese Weise verhält, ist eine Suchmaschine für Sniffing-Tools eine umfassende Lösung. Eine weitere Option ist, einen DNS-Server zu verwenden, welcher seine Antworten signiert.

Andere Möglichkeit des DNS-Missbrauchs

Es gibt eine weitere Angriffsart, welche einen DNS-Server ausnutzt. Diese Variante ist jedoch schon ziemlich alt und nur bei älteren DNS-Versionen von BIND-Servern (UNIX DNS-Servern) effektiv, man stößt jedoch immer noch manchmal darauf. Diese Angriffsart wird Cache Poisoning genannt und setzt auf die Unterwanderung einzelner autorisierter DNS-Antworten. Um diesen Trick ausführen zu können, benötigt der Hacker nicht einmal Zugriff auf das Netzwerk. Die Lösung, um ihn auszusperren, ist jedoch relativ simpel: ein Software-Update.

Routing und Weiterleitung

Routing bezieht sich auf die Eigenschaften des IP-Protokolls, welches managt, auf welchem Weg Pakete durch das Netzwerk geleitet werden – unter der Bedingung, dass die Systeme, in die sich der Hacker unterwegs einklinkt, Routing zulassen. Mittels Routing können Pakete leicht gefälscht werden, wodurch man unautorisierte Informationen erhalten kann. Die optimale Lösung bestünde darin, Routing auszuschalten (aber weder Windows noch Linux stellen diesen Service in der Regel zur Verfügung). Nichtsdestotrotz

sollte, so lange man Routing benötigt, die Zugriffssteuerungsliste (ZSL) in allen Routern korrekt eingestellt sein.

Andererseits ermöglicht es Routing einem Hacker, auf das interne Netzwerk zuzugreifen, welches durch ein System verbunden sein kann und nicht für das Internet, das es umgibt, sichtbar sein muss. Dies ist unter der Bedingung möglich, dass die Weiterleitungsregeln nicht adäquat entworfen sind. Deshalb sollte man die Regeln stets überprüfen und testen.

Session Hijacking

Das "Entführen" einer Kommunikationssitzung bezeichnet eine fortgeschrittenere Angriffsmethode: Der Hacker benötigt ein fundiertes Wissen über Netzwerkkommunikation, was diesen Angriff besonders gefährlich macht. Wie zuvor muss der Hacker den Netzwerkverkehr überwachen. Ein ausgeklügeltes Gerät zum Hijacking von Sitzungen nennt man Hunt. Der Hacker startet das Hunt-Programm auf seinem Computer und beobachtet die Kommunikation zwischen zwei Systemen. Nachdem er den idealen Moment für das Hijacking der Sitzung abgewartet hat, versucht er, die Kontrolle darüber zu erlangen. Ist er erfolgreich, bekommt er die volle Kontrolle über die Sitzung und das Zielsystem findet nicht heraus, dass es mit einem fremden Subjekt kommuniziert. Alles in allem ist der Hacker nun in der Lage, all das zu machen, was der ursprüngliche Sitzungsinhaber machen kann. Adäquat schützen kann man sich davor nur durch geeignete Verschlüsselung und erhöhte Netzwerksicherheit.

Man In The Middle

Unter diesen Attacken versteht man weniger ausgereifte Methoden, welche leicht verhindert werden können. Im Wesentlichen hängt ihr Erfolg von der Naivität und Unreflektiertheit der Nutzer ab. Solche Angriffe können auch über verschlüsselte Protokollen wie SSH oder SSL ausgeführt werden. Kurz gesagt handelt es sich um keinen Protokollfehler, sondern um einen Missbrauch des Nutzervertrauens.

SSH

Wie schon der Titel dieses Angriffs andeutet, besteht ihr Grundprinzip darin, ein Kommunikations-medium bereitzustellen. Der Hacker muss die Sitzung eines Clients kapern, eine Verbindung zum tatsächlichen Zielserver herstellen und vorgeben, das Ende-zu-Ende-System zu sein. Dadurch fällt einem Client nicht auf, dass er über ein Drittsystem kommuniziert. Es gibt jedoch ein kniffliges Detail: Fakt ist, dass jeder SSH-Server seinen eigenen Identifikationsschlüssel hat. Da der Hacker in der Regel diesen Schlüssel nicht besitzt, muss er die Sicherheitsvorkehrungen umgehen. In den meisten Fällen erstellt er hierzu seinen eigenen Schlüssel. Dies führt jedoch dazu, dass einem Client, der sich mit dem System des Hackers verbindet, eine Warnmeldung angezeigt wird, die ihn auf die Änderung des Schlüssels aufmerksam macht. Zusammenfassend kann man sagen, dass der Erfolg dieser Attacke von der Gleichgültigkeit und der Sorglosigkeit des Nutzers abhängt.

Nur dann, wenn ein Nutzer alle Warnungen ignoriert und ohne jede Skepsis weitermacht, wird einem Hacker die Möglichkeit gewährt, den Verkehr zu verfolgen. Sobald einem eine derartige Ungereimtheit auffällt, sollte man den Server-Administrator kontaktieren.

SSL

Der Angriff über ein Medium kann auch auf das SSL-Protokoll angewendet werden. Das Prinzip ist dasselbe. Allerdings ist diese Angriffsart sogar noch gefährlicher, da das SSL-Protokoll innerhalb der Website verwendet wird. Hiermit interagieren unerfahrene Nutzer, welche es von den grafischen Benutzeroberflächen moderner Betriebssysteme gewohnt sind, blind jeder angezeigten Nachricht zuzustimmen. Deshalb ist es sehr wichtig, SSL-Zertifikate daraufhin zu überprüfen, ob sie von einer offiziellen Zertifizierungsbehörde signiert wurde. Vorsichtig sollte man vor allem bei selbst signierten Zertifikaten sein.

Passwörter

Selbst dann, wenn ein Netzwerk vollständig gesichert ist, alle Nutzer sich an die Sicherheitsrichtlinien halten und alles sorgfältig überwacht, kontrolliert und analysiert wird, kann ein Netzwerk immer noch angegriffen werden. Die meisten Server bieten bestimmte Dienste an, ohne die das Internet nicht wunschgemäß funktionieren würde. Auf diese Dienste können verschiedene Nutzergruppen über ein Netzwerk zugreifen. Manche dieser Services können vielleicht sogar von jedem genutzt werden, andere jedoch nur von bestimmten Personen. Unabhängig davon, wem ein Dienst angeboten wird, kann ein Angriff in der Regel durch das Netzwerk ausgeführt wird. Hacker nutzen hierfür eine Reihe verschiedener Methoden und Tricks. Stellt sich jedoch heraus, dass ein Netzwerk vollkommen sicher ist und die meisten der gebräuchlichen Angriffe fehlschlagen, könnte ein Hacker dazu übergehen, sich die Passwörter vorzunehmen. Nun ist es zwar so, dass diese Angriffe relativ zeitaufwändig sind und nicht immer zum Erfolg führen. Nichtsdestotrotz handelt es sich hierbei um die letzte Möglichkeit, in das System einzudringen. Passwörter aller Protokolle, welche zu einer bestimmten Form der Authentifizierung dienen, können angegriffen werden, zB SMTP, POP, FTP, SSH usw. Dieser Angriff kann von dutzenden Geräten ausgeführt werden. Nachfolgend gibt es einen Überblick über die verschiedenen Methoden des Passwort-Ratens und wie man es verhindert.

Wörterbuchangriff

Ein Wörterbuchangriff ist die häufigste Methode, Passwörter zu raten. Er erfordert einen schnellen Prozessor, ein optimiertes Programm und ein langes Wörterverzeichnis. Mithilfe eines geeigneten Programms ist es möglich, fast alle Passwörter anzugreifen. Das Raten von Passwörtern bezieht sich jedoch nicht ausschließlich auf Attacken, die über das Netzwerk ausgeführt werden: Passwörter können auch lokal geraten werden, was von besonderen Erfordernissen und Umständen abhängt. Das Grundprinzip besteht darin,

ein Wort zu nehmen, dieses in geeigneter Form anzupassen (in Bezug auf den Algorithmus) und es mit dem originalen Passwort abzugleichen. Netzwerkdienste sind darauf ausgerichtet, das Passwort über das Netzwerk zu übermitteln (seine Form wird vom Protokoll vorgegeben). Ein Wörterbuchangriff wählt Wörter aus, die als Passwörter in Frage kommen, und speichert diese in einer Datei ab. In der Folge werden verschiedene Zeichenkombinationen ausprobiert. Einige Wörterbücher sind sehr umfangreich, weshalb es günstig ist, ein Passwort zu wählen, welches sich nicht in einem bestimmten Wörterbuch befindet.

Passworterstellung

Sie sollten versuchen, ein zufälliges Passwort zu generieren und sich dieses irgendwo aufzuschreiben. Anschließend machen wir einen Test, ob das Passwort sorgfältig ausgewählt wurde. Nun benötigen wire in Wörterbuch. Ich empfehle, dass Sie sich Wörterbücher von der Plattform http://www.phreak.org/html/wordlists.shtml herunterladen. Darin finden sie eine große Auswahl an Wörterbüchern aus verschiedenen Sprachen. Sie können Wörterbücher herunterladen, die nach Themen oder Sprachen sortiert sind. Ich empfehle Ihnen, sie alle herunterzuladen. Nun gilt es herauszufinden, ob das gewählte Passwort sich darin findet. UNIX zB nutzt grep mojeheslo slovnik. Nachfolgend erhalten Sie ein paar Hinweise, wie sich ein starkes Passwort erstellen lässt.

<u>Was ein Passwort enthalten sollte:</u>

- Kleinbuchstaben des englischen Alphabets a-z
- Großbuchstaben des englischen Alphabets A-Z
- Ziffern 0-9
- Satzzeichen wie *, #, @,] etc.
- Mindestens sechs Zeichen

<u>Was ein Passwort nicht enthalten sollte:</u>

- ein echtes Wort
- einen Namen
- eine Kombination aus Name (Wort) und Zahlen, zB honza52
- persönliche Informationen, Spitznamen, den Namen der Frau usw.
- Zahlen, die man mit jemandem oder etwas in Verbindung bringen könnte
- Geburtstage, Telefonnummern, Adressen usw.

Es ist notwendig festzuhalten, dass ein Passwort nicht zweimal verwendet werden sollte. Legt man zB mehrere E-Mail-Adressen an, sollte man für jede davon ein eigenes Passwort vergeben. Es könnte sein, dass ein Passwort herausgefunden wird (zB durch ein Sniffing-Tool). Dies würde einem Hacker die Möglichkeit geben, auf mehrere andere Systeme zuzugreifen.

14. LITERATUR

Habraken, Joseph W. Průvodce úplného začátečníka pro Počítačové sítě : není zapotřebí žádných předchozích zkušeností!. 1. vyd. Praha : Grada, 2006. ISBN 80-247-1422-1.

STALLINGS, William. Local and metropolitan area networks. 6th ed. Upper Saddle River: Prentice Hall, 2000. xvi, 478 s. ISBN 0-13-012939-0.

PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : [technologie pro datovou, hlasovou i multimediální komunikaci]. 2. aktualiz. vyd. Brno: Computer Press, 2006. 430 s. ISBN 8025112780.

THOMAS, Robert M. Lokální počítačové sítě. Vyd. 1. Praha: Computer Press, 1996. 277 s. ISBN 80-85896-45-1.