

Modul 16

1. Die Welt von Clients und Servern:

- **Aufgabe:** Begebe dich zu den weisen Datenhütern und erfahre, wie die Beziehung zwischen Client und Server in den Datenwolken funktioniert. Ergründe die Bedeutung von Softwareanwendungen, die als Server laufen, und Software wie Webbrowser, die als Clients fungieren können.

A: Der Unterschied wodurch sich Clients und Server unterscheiden, ist die Software was auf dem jeweiligen Gerät läuft. Server stellen Informationen bereit und Clients erfragen und darstellen diese Information. Die Beziehung zwischen Server und Client funktioniert wie folgt: ein Web-Server stellt seine Web-Seite mit einer öffentlichen IP bereit und einer Domain inkl. Portnummer. Der Client ruft nun den Web-Server mit der Domain auf, die wiederum erstmal von einem DNS-Server in die IP-Adresse identifiziert werden muss damit der Web-Server gefunden werden kann. Nachdem der Server gefunden wurde, wird eine TCP Verbindung aufgebaut mit dem jeweiligen Quell und Ziel Port. Nun passiert das typische Antwort-Frage Prinzip: Server antwortet dem Client mit Datenpaketen der Web-Seite. Der Client fragt ob alle Pakete da sind und sendet die Anzahl der Sequenznummer die erfolgreich übertragen worden sind und der Server schickt (wenn welche fehlen) die restlichen Segmente.

2. Die Magie von URIs:

- **Aufgabe:** Untersuche die Geheimnisse der URIs (Uniform Resource Identifiers). Lerne die Teile einer URI kennen, einschließlich Protokoll/Schemata, Hostname, Pfad und Dateiname. Erkenne die Unterschiede zwischen URN und URL und ihre speziellen Verwendungen.

A: Die URL (Uniform Resource Locator) definiert den Netzwerkstandort der bestimmten Ressource im Netzwerk. HTTP oder HTTPS URLs werden meistens von Webbrowser verwendet.

Die URN (Uniform Resource Name) gibt an welche Art von Inhalt die Webseite beinhaltet ohne das Protokoll anzugeben.

Eigenschaften einer URL sind wie folgt:

Protokoll (HTTP,HTTPS,SMTP,FTP)

Hostname (www.example.com)

Dateiname (/author/book.html)

Zusatz Eigenschaft (#page155)

3. **Dienste der Netzerkennung:**

- **Aufgabe:** Entdecke die häufigsten Internetdienste wie Internetrecherchen, soziale Medien, Video- und Audio-Streaming, Online-Shopping, E-Mail und Messaging. Verstehe, wie diese Dienste auf Protokollen aus dem TCP/IP-Protokollpaket basieren.

A: Das sind die meist genutzten Internetdienste:

DNS (identifiziert URLs in IP-Adressen)

SSH (Sichere Remote Sitzung zu Server und Netzwerkgeräte)

SMTP (wird zum Versenden von Mails und Anhänge benutzt)

POP u. IMAP (wird von Emailclient benutzt um Mails und Anhänge von einem Remote Server herunterzuladen)

DHCP (wird zur automatischen Adressierung von IP-Adressen)

in lokalen Netzwerken benutzt)

HTTPS (benutzt von Webbrowser um Webseiten von Webserver zu erfragen und dann mit den **HTML** Dateien die Webseite darzustellen)

FTP (wird für Datentransfer zwischen 2 Systemen benutzt)

4. Die Macht des DNS:

- **Aufgabe:** Reise zu den Tiefen des Domain Name Systems (DNS). Lerne, wie Hosts die IP-Adressen von Servern über DNS-Anfragen abrufen, und erfahre mehr über die Organisation von DNS-Namen im Internet.

A: Wenn ein Client über einen Webbrowser versucht eine Webseite mithilfe einer URL/Domainnamen wird nachdem diese Eingabe getätigt wurde die Anfrage erst einmal zu einem DNS Server gesendet um den jeweiligen Domainnamen in eine IP-Adresse zu identifizieren, weil nur IP-Adressen im Internet erkannt werden können.

5. Die Kunst der Webkommunikation:

- **Aufgabe:** Tauche ein in die Interaktion zwischen Webclients und -servern. Verstehe den Ablauf von Anfragen über HTTP und sichere Anfragen über HTTPS. Erforsche, wie Webseiten mithilfe von HTML codiert werden.

A: Wenn ein Client eine Webseite erfragt wird dieser über HTTP/HTTPS geliefert mit den entsprechenden HTML Dateien welche dann über den Webbrowser die Webseite darstellen. HTTP ist nicht sicher da die Verbindung vom Webserver zum Client abgefangen werden kann und von dritten gelesen und die Dateien verändert werden können. Deswegen wird

heutzutage empfohlen Webseiten nur mit dem HTTPS Protokoll aufzurufen.

6. FTP-Geheimnisse:

- **Aufgabe:** Reise zu den FTP-Servern und -Clients. Lerne, wie das File Transfer Protocol (FTP) den einfachen Austausch von Dateien ermöglicht. Verstehe die Verwendung von TCP-Ports 21 und 20 bei FTP-Sitzungen.

A: Port 21 wird vom FTP-Server und Client benutzt um den bevorstehenden Datenverkehr eine aktive Verbindung aufzubauen. Port 20 wird dann für die Übertragung der Dateien benutzt.

7. Die Welt der Virtuellen Terminals:

- **Aufgabe:** Entdecke die Welt von Telnet und Virtual Terminals. Verstehe, wie Telnet Textterminals über das Netzwerk emuliert, aber auch die Sicherheitsprobleme dabei. Vergleiche Telnet mit SSH und erfahre, warum SSH sicherer ist.

A: Virtuelle Terminals werden benutzt um Zugriff auf einen Server oder Netzwerkgerät aufzubauen, wie als würde man physikalisch am Gerät selbst sein. Seit den 1970s wurde Telnet benutzt um sogenannte "virtual terminal (vty) sessions" und läuft über TCP Port 23. Das Problem ist das diese Telnet Verbindung Dateien in Klartext überträgt. SSH hingegen verschlüsselt die Dateien.

8. E-Mail und Messaging:

- **Aufgabe:** Tauche ein in die Kommunikation über E-Mail und Messaging. Lerne die Protokolle SMTP, POP3 und IMAP4 kennen. Verstehe, wie E-Mail-Clients mit Mail-

Servern kommunizieren und wie Instant Messaging und VoIP die Kommunikation bereichern.

A: SMTP wird zum versenden von Emails benutzt über den Port 25. POP und IMAP wird zum Empfangen der jeweiligen Emails benutzt. Es wird eine Kopie der Mail vom Mailserver heruntergeladen. Bei POP (Port 110) wird sie nicht auf dem Server dann extra noch gespeichert unter IMAP (Port 143) wiederum schon.

Instant Messaging ist buchstäblich eine aktive Peer to Peer Verbindung. Beide Geräte können senden und empfangen. Genauso funktioniert auch VoIP (Voice over Internet Protokoll)