

## Aufbau eines Active-Directorys

### AD = (Active-Directory)

Verzeichnisdienst von Microsoft Servern

**Active Directory** ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern/abbilden.

Dient zur Verwaltung von verschiedenen Objekten in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften.

Ermöglicht dem Administrator die Informationen der Objekte zu organisieren, bereitstellen und zu überwachen.

Ein Active Directory ist in drei Komponenten aufgeteilt:

**Das Schema:** ist eine Schablone für alle Active-Directory-Einträge. Es definiert die Objekte, ihre Klassen und Attribute.

**Die Konfiguration:** beschreibt die Active-Directory-Gesamtstruktur und deren Bäume.

**Die Domain:** enthält schließlich alle Informationen, die sie selbst und die in ihre erstellten Objekte beschreiben.

Das Schema und die Konfiguration werden zwischen allen Domain Controllern der Gesamtstruktur repliziert.

Die Domain spezifischen Informationen sind nur innerhalb der jeweiligen Domain verfügbar.

Der Verbund mehrerer zusammengehöriger Domains heißt im englischen Original „forest“, deutsch „**Gesamtstruktur**“.

### Vorteile:

Zentrale Rechte- und Richtlinienverwaltung

Hohe Ausfallsicherheit durch Replikation

Zusammenarbeit mit anderen Verzeichnisdiensten

Einfach zu erweitern

Flexibel skalierbar

Unterschiedlichste Organisationsstrukturen abbildbar

Hohe Informationssicherheit

## Funktionsprinzip eines Domain-Controllers

Ist ein **Microsoft Server** zur zentralen **Authentifizierung** von **Computern** und **Benutzern** in einem **Netzwerk**.

In einem Netzwerk mit **Domain-Controller** können mehrere Computer zu einer **Domain** zusammengefasst werden.

Am **Domain-Controller** kann festgelegt werden, welche **Benutzer** sich mit welchem **Passwort** an der **Domain** anmelden dürfen, und zu welchen **Benutzergruppen** sie gehören.

Eine Domain ist lokaler Sicherheitsbereich mit zentraler Verwaltung der **Ressourcen** und stellt die administrative Grenze dar.

## **Kenntnisse über den Netzwerkdienst DHCP**

### **DHCP (Dynamic Host Configuration Protocol):**

Es ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server.

Beim Client muss lediglich automatischer Bezug der IP-Adresse eingestellt sein.

Konfiguriert werden kann, IP-Adresse, Subnetzmaske, Gateway, DNS-Server

Es können auch mehrere DHCP Server verwendet werden. Aber am besten mit getrennten Bereichen.

DHCP ist dynamisches BootP, kann auch BootP-Anfragen beantworten.

Keine fixe Zuordnung, kann flexibel IP-Adressen aus einem Adressen-Pool zuweisen und reservieren.

Die Zuweisung der IP-Adresse kann automatisch, dynamisch oder manuell erfolgen.

Einsatz in Server, Router.

### **BootP – Bootstrap Protocol:**

Erlaubt die Zuweisung einer IP-Adresse zu einem Endgerät (MAC-Adresse).

Die Adressen sind fest im Server eingetragen – keine flexible Zuweisung.

Überträgt für das Booten wichtige Informationen.

### **Betriebsarten:**

#### **Manuelle Zuweisung – Statisches DHCP:**

Ist eine feste Zuweisung von IP-Adressen zu MAC-Adressen.

Der Netzadministrator kann einem Client eine Adresse zuweisen bzw. reservieren, damit er immer die gleiche IP-Adresse erhält.

#### **Automatische Zuweisung:**

Dabei wird ein Adressbereich definiert.

Einmal zugewiesene Adressen sind fix reserviert.

Der Nachteil ist, wenn eine IP-Adresse nicht mehr verwendet wird, bleibt sie trotzdem reserviert und kann von einem anderen Client nicht verwendet werden. Wenn der gesamte Bereich vergeben ist, kann dann keine IP-Adresse mehr vergeben werden.

#### **Dynamischen Zuweisung:**

Funktioniert wie die automatische Zuweisung...

Dabei wird ein Adressbereich definiert, jedoch ist die IP-Adresse für den Client nur für eine gewisse Dauer reserviert, als für eine „Lease-Time“

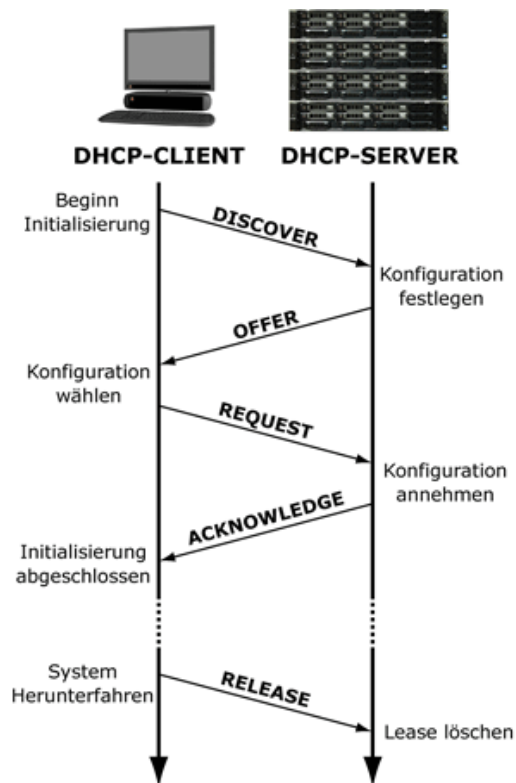
Die Lease Time bestimmt die Länge der Gültigkeit der Adress-Zuweisung. Der Client muss sich innerhalb der Lease-Time melden bzw. den Lease verlängern.

#### **Ausschlüsse:**

Es können auch IP-Bereiche von der DHCP Vergabe ausgenommen werden.

Um sie z.B. lokal für Server, Drucker, NAS, Storage, usw. zu vergeben.

## Phasen einer DHCP Zuweisung:



NACHRICHT	BESCHREIBUNG
DISCOVER	Broadcast eines Client, der einen Server sucht
OFFER	Antwort eines Servers mit einem Konfigurationsvorschlag
REQUEST	Broadcast des Clients an den bevorzugten Server. Ablehnung an alle anderen Server.
ACKNOWLEDGE	Der Server liefert eine IP-Adresse
NAK	Der Server lehnt die Anfrage des Clients ab
DECLINE	Der Client hat ein Problem mit der angebotenen IP-Adresse und lehnt ab.
RELEASE	Der Client gibt die IP-Adresse vor Ablauf des Lease zurück.



### DHCP Discover

Der Client sendet einen Broadcast (UDP - User Datagram Protocol).

### DHCP Offer

Der Server bietet Werte an.

### DHCP Request

Ack - Der Client fordert die angebotenen Werte an.

Reject - Der Client lehnt die angebotenen Werte ab.

### DHCP Acknowledge

Der Server bestätigt, und der Client empfängt die Netzwerkkonfiguration inkl. Lease Time und konfiguriert sich.

### DHCP Nack

Der Server lehnt ab.

### DHCP Decline

Ist eine Meldung des Client, wenn ein Fehler aufgetreten ist (z.B. IP-Konflikte,).

### DHCP Release

Der Client gibt die eigene Konfiguration frei, damit diese für andere Clients zur Verfügung stehen.

## **Funktionsprinzip eines Proxy-Servers**

### **Proxy Server = Stellvertreter**

- Ein Proxy stellt als Stellvertreter für den Client die Verbindung zum Webserver auf.
- Er ist ein Zwischenspeicher innerhalb eines Netzwerks.
- Er nimmt Anfragen von Clients an, wertet sie aus, und leitet stellvertretend die Anfrage ins Internet weiter.
- Zurückgelieferte Daten werden vor dem Weiterleiten am Proxy gespeichert. Bei erneuter Anfrage auf das gleiche Ziel werden die Daten nicht aus dem Internet geladen, sondern direkt vom Proxy Speicher zum Empfänger geschickt.
- Er kann Inhalte der Verbindungen überprüfen und ausfiltern/entfernen.

### **Vorteile:**

Spart Datenverkehr, senkt die Kosten und erhöht die Bandbreite für andere Anwendungen.

### **Einsatz:**

Attachments im E-Mails ausfiltern

Mail ohne Betreff ausfiltern

Mails mit bestimmten Inhaltswörter ausfiltern

Ausführbare Dateien in E-Mails ausfiltern

Inhalte prüfen/filtern/sperrern

Benutzerauthentifizierung

Logging/Caching

Herkunft verschleiern (TOR)

## **Funktionsprinzip eines Webserver**

### **Sind von Providern betriebene Server für das Webhosting.**

- Ist mit dem Internet oder Intranet verbunden
- Hostet eine Internetseite, die auf Anforderung eines Browsers, eines Clients, über HTTP oder HTTPS angefordert werden kann.
- Benötigt fixe IP-Adresse und DNS-Eintrag, um vom Internet erreichbar zu sein und zu bleiben.

### **Aufruf einer Webseite:**

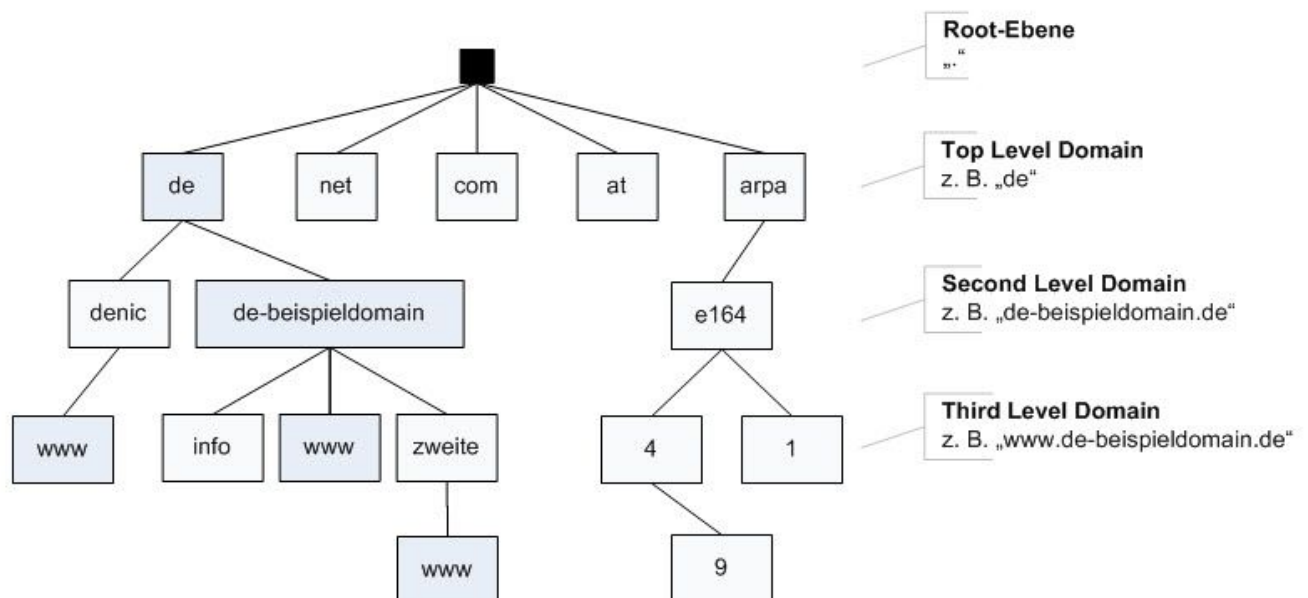
- Beim Client wird im Webbrowser eine Internetseite, www.google.at, eingegeben, und dadurch eine Anfrage zum DNS-Server gesendet.
- Der DNS-Server ermittelt zum Domainnamen (FQDN – Full Qualified Domain Name) die IP-Adresse des Webserver auf dem die Webseite liegt, und schickt diese an den Client.
- Danach baut der Client eine TCP-Verbindung zum Webserver auf, und sendet diesem eine Anforderung. Der Client stellt für jede benötigte Datei (Grafiken, Videos, ...) eine eigene Anfrage.
- Der Webserver schickt dann die angeforderten Dateien an den Client, der diese dann am Bildschirm im Webbrowser darstellt.
- Nach Erhalt der kompletten Webseite wird die TCP Verbindung abgebaut.

## Kenntnis des DNS-Dienstes und dessen hierarchischen Aufbaues

### DNS (Domain Name System):

#### Aufbau:

- Das DNS ist ein weltweit auf tausenden von Servern verteilter hierarchischer Verzeichnisdienst zur Umwandlung von Rechnernamen in IP-Adressen.
- Es gibt keine zentrale Datenbank.
- Die DNS-Datenbank – Zuweisung eine in Zonen aufgeteilte baumförmige Struktur.
- Die Wurzel ist das Root-Verzeichnis. Darunter befinden sich die Top Level Domains (TLDs) (.com, .org, net), dann die Second Level Domains (co.uk) (für kommerzielle Unternehmen in England), und dann die Sub Domains.



#### Aufgabe:

- Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.
- Das DNS funktioniert ähnlich wie eine Telefonauskunft.
- Der Benutzer gibt im Browser einen Domain-Namen ein, z.B. [www.google.at](http://www.google.at)
- Der Browser fragt dann einen DNS-Server, der in der IP-Konfiguration hinterlegt ist.
- Die DNS-Anfrage wird dann vom DNS-Server in die zugehörige IP-Adresse umgewandelt, und führt so zum richtigen Rechner.
- Wird der Domain-Name nicht aufgelöst, kann auch keine Verbindung zum Host aufgebaut werden. Außer der Benutzer weiß die IP-Adresse des Ziel Hosts.

## Fachbegriffe Domain, Sub-Domain und Top-Level-Domain

#### Domain:

- Eine Domain ist ein Teilbereich des DNS (Domain Name System)
- Eine Domain hat einen weltweit eindeutigen Namen
- Ein Domänenname ist die Bezeichnung für ein Netzwerksegment
- Eine Domain bezeichnet die Adresse, unter der eine Webseite im Browser aufgerufen werden kann.

- Die komplette Adresse wird FQDN genannt (Full Qualified Domain Name)

Sie setzt sich zusammen aus:

- Top-Level-Domain
- Second-Level-Domain bzw. Domain
- Third-Level-Domain bzw. optionalen Subdomains und Hostnamen
- Zum Beispiel foto.abc.com
- Die maximale Namenlänge beträgt 63 Zeichen pro Ebene/Label (63 für Domain und 63 für Sub Domain, ...). Gesamt 255 Zeichen.
- Die Regeln für die Namensvergabe legt die Vergabestelle NIC (Network Information Center) der jeweiligen Top Level Domains fest.

Beispiel:

- <http://www.foto.abc.com>
- http = Übertragungsprotokoll
- foto = Third-Level-Domain oder Sub Domain
- abc = Second-Level-Domain oder Domain
- com = Top-Level-Domain
- Sub-Domain ist der vorderste Teil der Domain-Adresse (www.foto.abc.com)  
Sie liegt in der Hierarchie unterhalb einer anderen Domain
- Second-Level-Domain ist der Domain Name und steht vor der Top-Level-Domain (www.foto.abc.com)
- Top-Level Domain ist der letzte Teil der Domain-Adresse (www.foto.abc.com)

## Kenntnis der Web-Protokolle HTTP und HTTPS

HTTP (Hyper Text Transfer Protocol):

- Einsatzbereich
- Wird zur Web-Kommunikation im Internet und Intranet eingesetzt.
- Sorgt für einen reibungslosen Transport von HTML-Seiten zwischen Webserver und Web-Client.
- Wichtigsten Funktionen sind Dateien vom Webserver anzufordern und zum Browser zu schicken.
- Browser übernimmt die Darstellung von Texten und Bildern.
- Adressierung

URL (Uniform Resource Locator) setzt sich zusammen aus:

- Protokollangabe
- Portadresse des Kommunikationsprotokolls
- Pfadangabe
- Name des Dokuments

`http://www.microsoft.com:80/windows/index.htm`

Protokoll                      Host                      Port                      Pfad

HTTPS (Hypertext Transfer Protocol Secure):

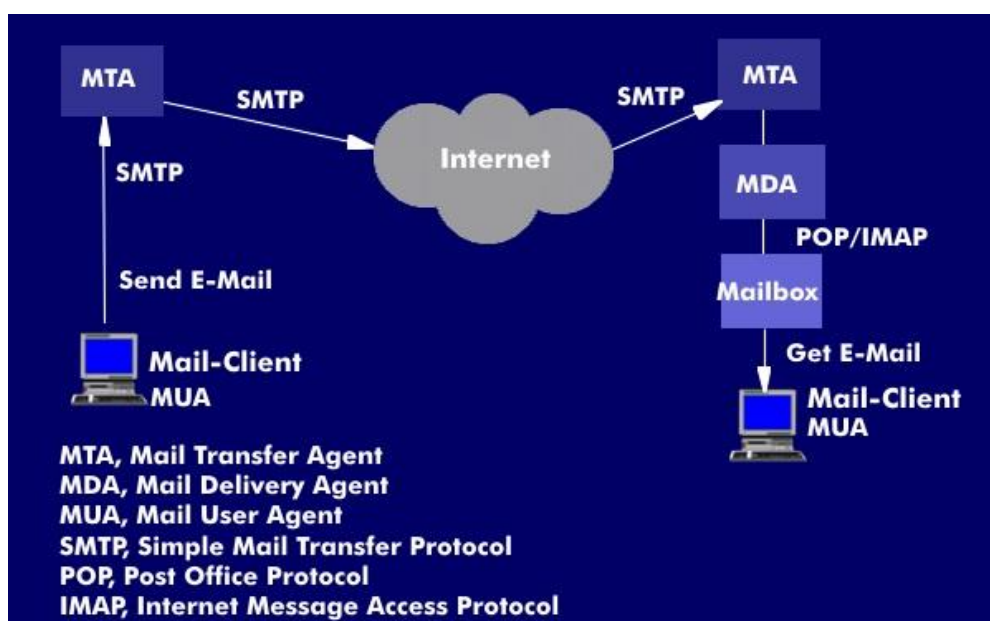
- Benutzt zusätzlich eine Verschlüsselung zur Übertragung. (SSL - Secure Socket Layer, TLS - Transport Layer Security)
- Daten werden sonst als Klartext unverschlüsselt übertragen.
- Einsatz bei Webserver, Authentifizierung auf Webseiten.
- Ziel ist die Verhinderung von Man in the Middle Angriffe und Phishing.

## Funktionsprinzip eines Mail-Servers

Ein Mail-Server ist eine Software, die Nachrichten und Mitteilungen:

- empfangen,
- senden,
- zwischenspeichern
- und weiterleiten kann.
- Die Nachrichten können von E-Mail-Clients abgerufen und bearbeitet werden.
- Mail-Server fungieren als Mail Transfer Agent (MTA), die die gespeicherten Nachrichten mit dem Simple Mail Transfer Protocol (SMTP) zum nächsten Mail-Server weiterleiten, bis hin zu dem Mail-Server, in den sich der empfangende Benutzer mit seiner E-Mail-Adresse eingeloggt hat.
- Benutzer können über ihren E-Mail-Account mit der E-Mail-Adresse auf E-Mail-Server zugreifen.
- Die Mail-Adresse beinhaltet die Hostadresse, häufig die eines Providers, und die Länderkennzeichnung, die Top Level Domain (TLD).
- Die von einem E-Mail-Client an einen E-Mail-Server gesendeten E-Mails werden so lange zwischengespeichert, bis sie vom Empfänger abgeholt werden.
- Dies erfolgt mit dem Post Office Protocol (POP) oder dem Internet Message Access Protocol (IMAP).
- Der E-Mail-Client muss sich über seinen E-Mail-Account in seinen Mail-Server einloggen.

Funktionsweise:



MUA - Mail User Agent  
SMTP - Simple Mail Transfer Protocol  
MTA - Mail Transfer Agent  
MDA - Mail Delivery Agent  
POP - Post Office Protocol  
IMAP - Internet Message Access Protocol

#### Mögliche Fehler:

- Die Zieldomain ist falsch bzw. nicht vorhanden.
- MX-Record fehlt bzw. ist falsch.
- Zielmailserver ist offline.
- Benutzer ist nicht vorhanden.
- Mailbox ist voll, max. Mailgröße wurde überschritten.
- Spamschutz, Inhaltsschutz, Virenschutz, ...

#### SMTP-Relay-Server:

- Mail-Relay-Server/Smarthost
- Bezeichnung für einen MTA, der von einem Sender (A) E-Mails annimmt und an beliebige Dritte (C) weiterleitet
- A > RELAY > C

Ein korrekt konfigurierter SMTP-Relay-Server leitet E-Mails nur dann weiter, wenn er

- Entweder für A zuständig ist.
- oder/und für E-Mails an C zuständig ist.

### **Kenntnis der Mailprotokolle POP3/POP3S, IMAP/IMAPS und SMTP/SMTPS**

#### POP3 (Post Office Protocol):

- Einfaches Protokoll zum Herunterladen von E-Mail-Nachrichten von einem Mailserver.
- Die E-Mails werden, nachdem sie vom Server in den lokalen Mailspeicher geladen wurden, normalerweise vom Server gelöscht.
- E-Mail-Speicher am Client (geringer Speicherplatzbedarf am Server).
- Lösung grundsätzlich für Zugriff mit einem Client.

#### Vorteile:

- Onlineverbindung nur zum E-Mail-Download notwendig.

#### Nachteile:

- Alle E-Mails müssen vollständig heruntergeladen werden (FIFO – First In, First Out)
- Inkonsistenzen bei mehreren Clients
- Keine Ordnerstruktur am Server

#### POP3 und IMAP4 Gemeinsamkeiten:

- Authentifizierung am Server notwendig
- SMTP zum E-Mail-Versand notwendig
- SSL/TLS-Unterstützung
- E-Mail-Backup notwendig (Client, Server)

#### POP3S (Post Office Protocol Secure):

- Benutzt zusätzlich eine Verschlüsselung zur Übertragung. (SSL, TLS)
- Üblicherweise auf Port 995.



## IMAP/IMAPS:

### IMAP 4 (Internet Message Access Protocol):

- Komplexes Protokoll zum direkten Arbeiten auf dem Mailserver
- Die E-Mails werden auf dem Client nur angezeigt, wenn eine Netzwerkverbindung zum Mailserver besteht.
- Auf dem Client werden die E-Mails in der Regel nicht gespeichert.
- E-Mail-Speicher am Server (Speicherplatzbedarf am Server).
- Lösung für Zugriff mit mehreren Clients.

### Vorteile:

- Selektiver Download möglich.
- Mehrere Clients möglich (Synchronisation).
- Ordnerstruktur am Server möglich.

### Nachteil:

- Dauernde Onlineverbindung notwendig. (Offlinesynchronisation möglich)

### IMAPS (Internet Message Access Protocol Secure):

- Benutzt zusätzlich eine Verschlüsselung zur Übertragung. (SSL, TLS)
- Verwendet bereits beim Verbindungsaufbau zum Server SSL Verschlüsselung.

## SMTP = (Simple Mail Transfer Protocol):

Das SMTP- ist der Internet-Standard zur Verteilung von E-Mails.

### Die SMTP-Nachricht besteht aus:

- Header
- Received (Zeile über die Auslieferung je Transportservice)
- Message-ID
- From
- To
- Subject
- Date
- MIME-Version
- Content-Type

### Nutzdaten:

- ASCII-Text
- SMTP-Relay Server (Mail Relay Server, Smarthost)

### Ein korrekt konfigurierter SMTP-Relay-Server B leitet E-Mails nur weiter, wenn er:

- Entweder für Mails von A zuständig ist.
- Oder/Und für Mails an C zuständig ist

### SMTPS ((Simple Mail Transfer Protocol Secure):

- Benutzt zusätzlich eine Verschlüsselung zur Übertragung. (SSL, TLS).

## Kenntnisse über FTP/FTPS

### FTP (File Transfer Protocol):

- Dient zum Dateitransfer zwischen verschiedenen Systemen, und ist unabhängig von Betriebs- und Filesystem
- Nutzt den Client-Server Betrieb über TCP
- Nutzt die Benutzerauthentifizierung und Rechteverwaltung (Übertragung im Klartext)
- FTP Sitzung standardmäßig über Port 21.
- Ist eine unverschlüsselte Übertragung
- Arbeitet auf OSI Schicht 7

### Sonderfall - anonymous-FTP:

- ermöglicht den nahezu freien Zugang zu öffentlich betriebenen FTP Servern.
- für Nutzer ohne Konto
- Verbindung zum Server (Login > Username: anonymous, Passwort: „wird nicht überprüft“)

### FTPS (File Transfer Protocol over SSL):

- hierbei wird die FTP-Verbindung mit SSL oder TLS verschlüsselt.
- 2 verschieden Modus möglich:

#### Expliziter Modus

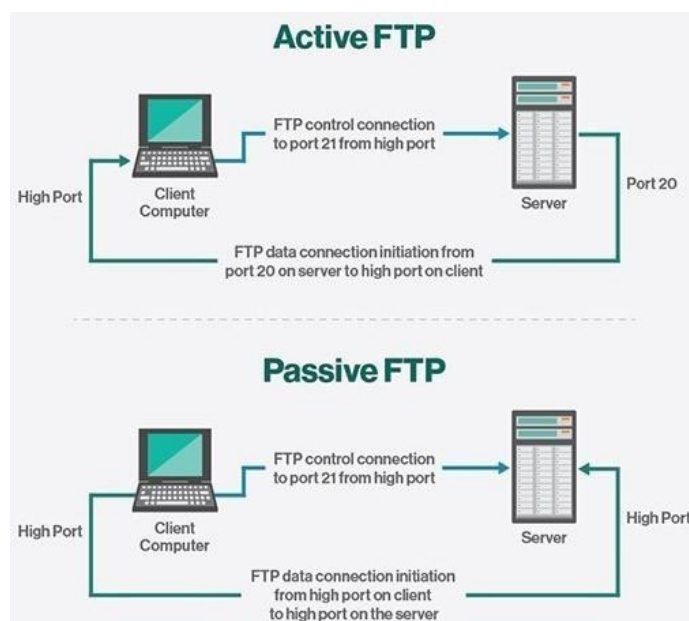
Der Client fordert vom Server an eine verschlüsselte Verbindung zu verwenden, die beide dann akzeptieren. Wenn der Client keine Verschlüsselung anfordert, kann der Server die unverschlüsselte Verbindung akzeptieren, oder er kann die Verbindung drosseln oder blockieren.

#### Impliziter Modus

Eine verschlüsselte Verbindung ist zwingend. Der Server antwortet nach einer Anfrage vom Client bereits verschlüsselt. Erhält er dann keine Antwort vom Client, wird er die Verbindung blockieren.

#### Aktives / Passives FTP:

- Für die FTP Verbindung wird immer ein Steuerkanal und ein Datenkanal benutzt.
- Der Client gibt immer vor ob eine Aktive oder Passive FTP Verbindung aufgebaut wird.



### Aktives FTP:

- Der Client öffnet einen beliebigen freien Port, jenseits von 1023, und baut über Port 21 den Steuerkanal auf. (für die FTP-Kommandos)
- Der Server baut von Port 20 den Datenkanal auf und sendet die Daten an den Client. (Datenübertragung)

### Passives FTP:

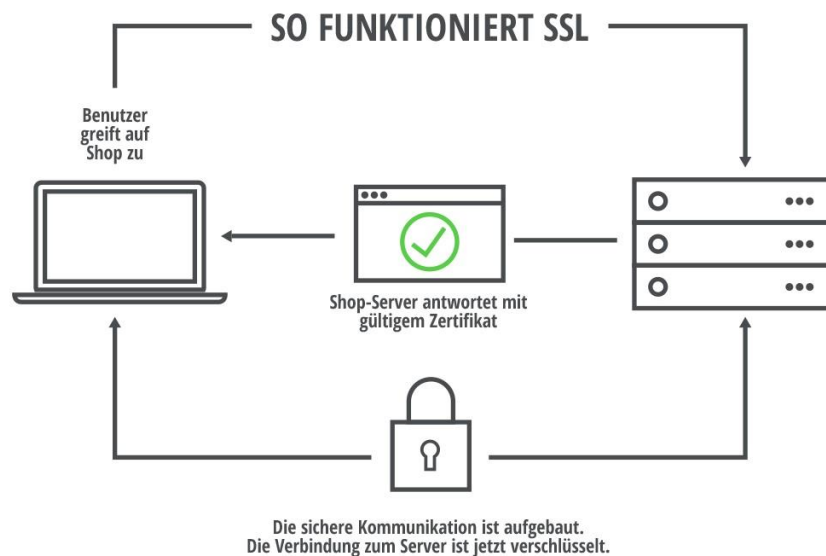
- Der Client öffnet einen beliebigen freien Port, jenseits von 1023, und baut über Port 21 den Steuerkanal auf.
- Der Client baut über einen beliebigen freien Port, jenseits von 1023, den Datenkanal auf und holt sich die Daten vom Server.
- Wird verwendet, wenn der Server den Client nicht erreichen kann (Client hinter Router, Firewall).

## Kenntnisse über SSL

### SSL (Secure Socket Layer):

- ist ein Protokoll für die Authentifizierung und Verschlüsselung von Internetverbindungen.
- Unternehmen lässt sich von einer Zertifizierungsstelle ein Zertifikat ausstellen. Dient als Ausweis für den Eigentümer einer Webseite. Wird z.B. auf einem Webserver hinterlegt. Liegt auch bei der Zertifizierungsstelle.
- Weiterentwicklung wurde mit Version 3 beendet.
- Aktuelles Verfahren ist [TLS \(Transport Layer Security\)](#).

### Funktionsweise:



- Es erfolgt eine Zertifizierung des öffentlichen Schlüssels des Servers bei der Zertifizierungs- und Validierungsstelle.
- Der Client sendet einen SSL-Request an den Server.
- Der Server authentifiziert sich mit dem Zertifikat.
- Dann lässt der Client das übermittelte Zertifikat bei der Zertifizierungs- und Validierungsstelle überprüfen/validieren. Ist es vertrauenswürdig sendet der Client eine Nachricht an den Server

- Dann sendet der Server eine Bestätigung, um die verschlüsselte Verbindung zu beginnen.

#### Einsatz:

- gesicherte Abruf von vertraulichen Daten über HTTP.
- gesicherte Übermittlung von vertraulichen Daten an den HTTP-Server.
- E-Mail, Browser - Webserver (Online-Banking, Online-Shopping)

### **Fachbegriff Cloud-Computing und Beispiele für marktbekannte Cloud-Dienste**

#### Cloud-Computing:

- Ist die Bereitstellung von Computerdiensten (Server, Speicher, Datenbanken, Netzwerkkomponenten, Software, Analyse- und intelligente Funktionen etc.) über das Internet.
- Stellt eine IT-Infrastruktur zur Verfügung, ohne dass diese auf dem lokalen Rechner installiert sein müssen.
- Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich durch technische Schnittstellen und Protokolle, etwa mittels eines Webbrowsers.

#### Gründe für Cloud-Computing:

- Kostensenkung
- Geschwindigkeit
- Globale Skalierung
- Leistung
- Produktivität
- Sicherheit

#### Beispiele für marktbekannte Cloud-Dienste:

##### Google Drive

Google Drive ist der Onlinespeicherplatz der bekannten Suchmaschine. Die Cloud-Dienste sind über den Browser und einem virtuellen Laufwerk erreichbar.

#### Vorteile:

- Wie bei allen Cloud-Diensten bietet der Cloud-Dienst die Möglichkeit, von verschiedenen Geräten auf den Speicher zuzugreifen. Der Zugriff auf die Daten erfolgt mit Hilfe eines virtuellen Laufwerks.
- Es stehen Ihnen 15 GB kostenloser Speicherplatz zur Verfügung. Kostenpflichtig stehen insgesamt 16 Terabyte Daten zur Verfügung.
- Die Daten lassen sich nicht nur im virtuellen Laufwerk, sondern auch über den Browser abrufen.
- Ein weiterer Vorteil ist die Suche. Bei der Eingabe eines Suchbegriffs werden sämtliche relevanten Dateien aus allen Bereichen angezeigt.

#### Nachteile:

- Der Anbieter ist teurer als die Konkurrenz
- Google Drive bietet keine 256-Bit Verschlüsselung an
- Die 15 GB Speicherplatz werden auch auf die anderen Dienste (Google Mail, Google+) angerechnet.

##### Dropbox

Die Dropbox gehört zu den Cloud-Diensten, die sehr einfach zu bedienen sind. Einfach nach der Anmeldung die Software auf dem Rechner installieren. Die Daten werden einfach in dem Ordner abgelegt. Es erfolgt eine automatische Synchronisierung mit dem Server.

Der kostenlose Speicherplatz beträgt 2 Gigabyte. Mehr Speicher – Kostenpflichtig.

#### Vorteile:

- Dropbox gehört zu den günstigsten Anbietern auf dem Markt
- Die Bedienung ist einfach und macht selbst Anfängern keine Probleme
- Es steht ein Support in deutscher Sprache zur Verfügung
- Die Daten lassen sich einfach und unkompliziert teilen

#### Nachteile:

- Es stehen nur 2 Gigabyte kostenloser Speicherplatz zur Verfügung.
- Die Daten befinden sich auf Servern in den USA.
- Bisher gibt es noch keine Office Funktionen.
- Es gibt keine externen Schnittstellen.

#### Microsoft OneDrive

ist der Speicherplatz für Windows- und Office-Anwender.

Wer Windows auf seinem Rechner installiert, bekommt die Anwendung gleich mitgeliefert.

Das Besondere am Cloud-Speicher OneDrive ist die enge Verzahnung mit Microsoft Office.

Wer sich Office 365 kauft, bekommt ein Terabyte an Speicherplatz und natürlich das Programmpaket.

#### Vorteile:

- Für Office Kunden unschlagbar günstig, da Office im Angebot enthalten ist
- Einfache Handhabung, da die Anwendung schon in Windows integriert ist
- Office-Programme haben den Cloud-Speicher integriert, sodass schon während der Arbeit eine Speicherung der Daten erfolgt.

#### Nachteile:

- Der kostenlose Speicherplatz beträgt nur 5 Gigabyte. Im Vergleich zur Konkurrenz ist das sehr wenig.
- Der Server von Microsoft OneDrive befindet sich in den USA.
- Viele Kunden möchten ihre Daten nicht in die Hände eines amerikanischen Herstellers legen. Daher führte Microsoft in Zusammenarbeit mit seinem Partner Telekom die sogenannte Microsoft Cloud Deutschland ein.

#### Amazon Cloud Drive

gibt es in zwei Varianten:

- Prime Kunden von Amazon bekommen automatisch 5 Gigabyte Cloudspeicher zugewiesen.
- Wer nur Fotos hochlädt, bekommt sogar unbegrenzten Speicherplatz. Das gilt aber nur für Fotos, nicht für Videos.
- Für einen Jahresbetrag von aktuell 70 Euro bekommt der User unbegrenzten Speicherplatz. Das ist im Vergleich zur Konkurrenz sehr günstig.

#### Vorteile:

- Im Vergleich zur Konkurrenz sehr günstig.
- Für Prime Kunden unbegrenzter Fotospeicherplatz.
- Einfache Handhabung der Software.

#### Nachteile:

- Das Teilen der Inhalte ist stark eingeschränkt.
- Nur wenig Hinweise auf den Datenschutz.
- Gelöschte Inhalte können nur 30 Tage wiederhergestellt werden.
- Mit der mobilen App können keine Videos und Fotos automatisch hochgeladen werden.

## iCloud Drive

- Beim Cloud-Speicher iCloud Drive handelt es sich um ein Angebot der Firma Apple.
- Die Software befindet sich auf Geräten, die das Apple-Betriebssystem iOS benutzen und ist vorinstalliert.
- Der Speicher kann darüber hinaus auch von Windows-Nutzern verwendet werden.
- Der freie Speicherplatz ist mit fünf Gigabyte sehr wenig.
- Hinzu kommt, dass dieser nicht allein für die Daten verwendet wird. Auch gespeicherte Fotos und die Datensicherung des iPhones verbraucht Speicherplatz.
- Wem der Speicher nicht reicht, kann noch zusätzliche Kapazitäten kaufen.

### Vorteile:

- Fester Bestandteil des Apple Betriebssystems
- Kann auch für Windows verwendet werden
- Einfache Handhabung

### Nachteile:

- Wenig Speicherplatz
- Speicherplatz wird auch von anderen Diensten benötigt.

## **Kenntnisse über Private/Public/Hybrid-Cloud**

### Public Cloud:

- Eine öffentliche Cloud befindet sich im Besitz eines externen Cloud-Diensteanbieters und wird von diesem ausgeführt, und für jeden zugänglich ist.
- Die Daten werden, im Gegensatz zur „Private Cloud“, nicht auf den Servern im Unternehmen gespeichert.

### Private Cloud:

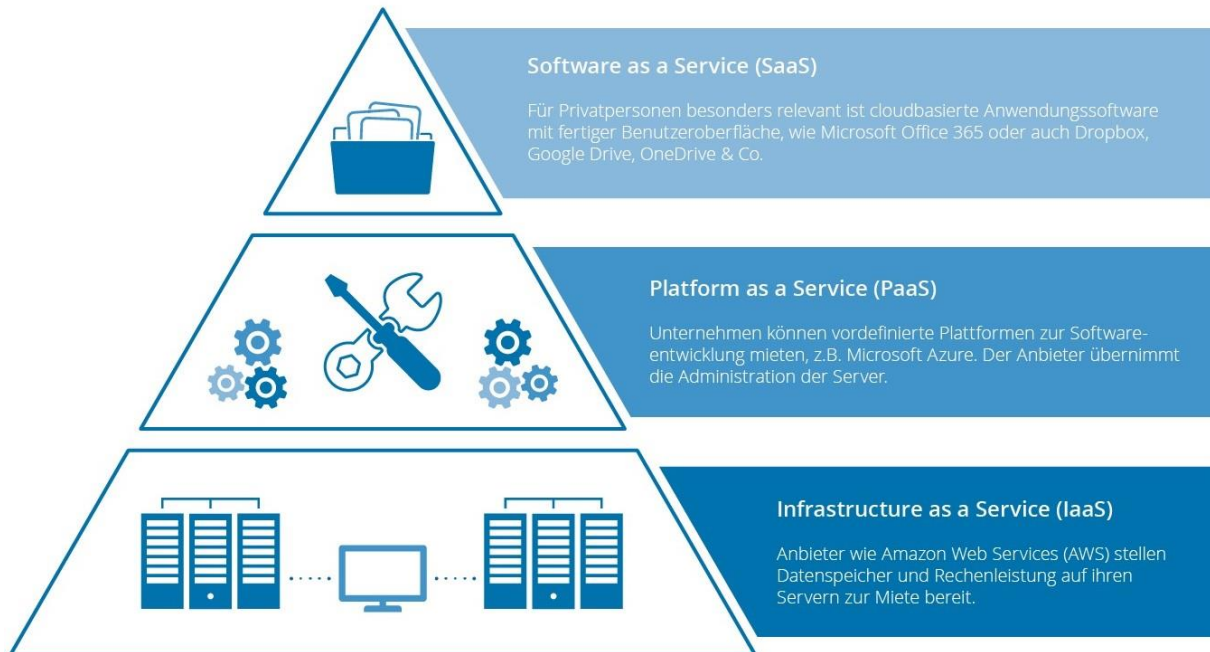
- Eine private Cloud wird exklusiv von einem einzigen Unternehmen genutzt.
- Wegen Datenschutz und Sicherheit ihre IT-Dienste betreibt das Unternehmen die Cloud selbst, um sie dann ihren Mitarbeitern zugänglich zu machen.
- Kann aber auch durch Dritte gehostet und verwaltet werden.

### Hybrid-Cloud:

- Ist eine Mischung aus Public und Private Cloud. Bestimmte Services laufen bei öffentlichen Anbietern über das Internet.
- Datenschutzkritische Anwendungen und Daten werden im Unternehmen betrieben und verarbeitet.

## Fachbegriffe IaaS, PaaS, SaaS

Es gibt unterschiedliche Arten von Cloud Computing. Eine mögliche Gliederung ist der technische Cloud-Stack, mit drei Schichten, in der obere Schichten auf den unteren Schichten aufbauen können, es aber nicht müssen.



### Infrastructure as a Service (IaaS):

- Ist die unterste Schicht der Cloud-Modelle.
- Ein externer Anbieter stellt grundlegende IT-Ressourcen wie Rechenleistung, Storage oder Netzwerkkapazitäten zur Verfügung.
- Der Anwender hat dabei die Kontrolle über Betriebssysteme und Anwendungen, er muss in der Regel die Infrastruktur selbst aus den benötigten Recheninstanzen (Server) und Speichern zusammenstellen. Sprich, der Anwender mietet sich IT-Infrastruktur und Wartung.

**Vorteil:** Skalierbarkeit, Benutzer hat Vollzugriff auf die Instanzen.

**Beispiel:** Amazon Web Services, Open Telekom Cloud

### Plattform as a Service (PaaS):

- Ist die mittlere Schicht der Cloud-Modelle.
- Ist eine Dienstleistung, die in der Cloud eine Computer-Plattform für Entwickler von Webanwendung zur Verfügung stellt.
- Anbieter stellt benötigte Ressourcen wie Rechenleistung, Speicher, Netzwerk zur Verfügung.
- Ermöglicht es Entwickler auf der angebotenen Infrastruktur mittels Schnittstellen eigene Programme zu entwickeln und auszuführen.
- Entwickler hat keinen direkten Zugriff auf die bereitgestellte Infrastruktur.
- Entwickler kann nur selbst eingebrachte Programme und Daten kontrollieren.

### Software as a Service (SaaS):

- Ist die oberste Schicht der Cloud-Modelle.
- Software und IT-Infrastruktur werden bei einem externen Anbieter betrieben und vom Kunden gegen Entgelt genutzt.

- Ausführung der Software durch Benutzung eines internetfähigen Computers und eines Internetbrowsers.
- Software muss beim Kunden nicht installiert werden, sondern wird „angemietet“.
- Kunde muss sich nicht um die IT-Infrastruktur und Updates der Anwendung kümmern.

#### Beispiele für marktbekannte Cloud-Dienste:

Webmail-Dienste, Google Drive, OneDrive, Microsoft Office 365, SAP, Apple iCloud.

### **Kriterien und Voraussetzungen für den Einsatz von Cloud-Diensten**

#### Kriterien:

- Kosten/Nutzen Faktor
- Datenschutz, Datensicherheit
- Verfügbarkeit und Performance
- Fehlerbehebung
- Service und Support
- Demand- und Kapazitätsmanagement
- Integration in das lokale Betriebssystem und Netzwerkinfrastruktur

#### Voraussetzungen:

- Unterstützung durch Management und Mitarbeiter
- Eine schnelle Breitbandverbindung
- Anpassung der IT-Strategie
- Aufbau von Entscheidungskompetenz
- Anforderungen des Unternehmens an die IT-Lösung
- Anforderung der Behörden