



Unternehmen für Bildung.

Netzwerke und Dienste bereitstellen

Modul: **ITFST / J**

Version: 1.0
Oktober 2022

Erstellt von: IT-Abteilung

Modul: **ITFST / J - Netzwerke und Dienste bereitstellen**

Version, Datum: 1.0, Oktober 2022

Erstellt von: IT-Abteilung

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Modulunterlage und alle ihre Bestandteile wurden mit großer Sorgfalt erstellt und geprüft. Dennoch können Fehler nicht vollkommen ausgeschlossen werden. Der Herausgeber und die Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Literaturhinweis

Titel: IT-Berufe Grundstufe

ISBN: 978-3-14-220000-2

Verlag: Westermann Gruppe

Inhalt

TAG 1 und TAG 2 - Netzwerkbereitstellung nach unterschiedlichen Unternehmensanforderungen unterscheiden	6
LE 1 - Kundenanforderungen formulieren	6
LE 2 - Einsatzgebiete	7
LE 3 - Betriebsmodelle	7
LE 4 - Erstgespräche mit Kunden	8
LE 5 - Lastenhefterstellung	11
LE 6 - Pflichtenhefterstellung	14
TAG 3 - Mit DevOps Netzwerkbereitstellung unterstützen	19
LE 1 - Ist-Analyse durchführen und Lastenhefte erstellen	22
LE 2 - Kleine Netzwerke für Kleinunternehmen planen	22
LE 3 - Mittlere Netzwerke für KMU und mittelgroße Organisationen planen	24
LE 4 - Große Netzwerke für Mittel- und Großunternehmen planen	25
TAG 4 - Technische Anforderungen für das Bereitstellen von Netzwerken berücksichtigen	27
LE 1 - Internet-Protokolle unterscheiden	27
LE 2 - IP Subnetting und virtuelle LANs (VLAN)	33
TAG 5 - Netzwerkkomponenten unterscheiden	39
LE 1 - Access Points	39
LE 2 - Firewall	40
LE 3 - DNS-Filter	42
LE 4 - Switches	43
LE 5 - VoIP-Telefonanlage	44
LE 6 - Repeater	45
LE 7 - Router	45
LE 8 - Gateway	48
TAG 6 - Server-Software unterscheiden	50
LE 1 - Server-Virtualisierung mittels virtueller Maschinen und Containern	50
LE 2 - Software as a Service (SaaS)	52
LE 3 - Webhosting	53
LE 4 - Infrastructure as a Service (IaaS)	54
TAG 7 - Server-Hardware unterscheiden	58
LE 1 - Dedicated Server/Bare Metal	58
LE 2 - Virtual Dedicated Server (VDS)	59
LE 3 - Virtual Private Server (VPS)	59
LE 4 - Network Attached Storage (NAS)	60
TAG 8 - Technische Anforderungen der Rechenzentren kennen	62
LE 1 - NAS - SAN - DAS	63
LE 2 - Unterbrechungsfreie Stromversorgung (USV)	63
LE 3 - WAN-Infrastrukturen unterscheiden	64
TAG 9 - Wirtschaftliche und sicherheitsrelevante Anforderungen sowie Nachhaltigkeit in Netzwerken berücksichtigen	68
LE 1 - Wirtschaftliche Anforderungen berücksichtigen	68

LE 2 - Make- or Buy-Entscheidung	68
LE 3 - Anschaffungs- und Betriebskosten	68
LE 4 - Kalkulation, Angebotsvergleiche und Finanzierung	70
TAG 10 und TAG 11 - Sicherheitsrelevante Anforderungen berücksichtigen.....	74
LE 1 - Schutzbedarf für Netze analysieren	74
LE 2 - Netzwerkarchitektur sicher planen	75
LE 3 - Netzarchitektur und -design, technisch-organisatorische Netzwerkmaßnahmen planen	77
LE 4 - Cloud-, Filial- und Betriebsanbindungen über Software Defined Networking.....	81
LE 5 - Nachhaltigkeit sicherstellen	85
TAG 12 - Pflichtenhefte nach Unternehmensanforderungen erstellen	88
LE 1 - Ausschreibungs- und Vergabeplanung	88
LE 2 - Funktionale Anforderungen planen	92
LE 3 - Netzwerk	92
LE 4 - Netzwerkkomponenten planen.....	99
LE 5 - Server	101
LE 6 - Nicht funktionale Anforderungen planen	102
TAG 13 - Netzwerke installieren, konfigurieren und bereitstellen	105
LE 1 - Infrastruktur einrichten.....	105
LE 2 - Netzwerkkomponenten installieren	107
LE 3 - Server installieren (klassisch)	109
LE 4 - E-Mail-Server für den Nachrichtenversand konfigurieren	113
LE 5 - Härten des Servers	113
TAG 14 - Funktionsprüfungen und Messungen durchführen, Dokumentationen erstellen	115
LE 1 - Prüfung der Infrastruktur	115
LE 2 - Prüfung der Netzwerkkomponenten.....	115
LE 3 - Vorstellung des Virtualisierungskonzeptes im Leistungsportfolio	119
LE 4 - Ausblick geben: Marktplätze für Container und virtuelle Anwendungen.....	125
TAG 15 - Vertiefung des Wissens und Modulprüfung	127
LE 1 - Einleitung.....	127
LE 2 - Modulprüfung	127

Netzwerke stellen Benutzern Anwendungen und Daten zur Verfügung, bieten die gemeinsame Nutzung vernetzter betrieblicher Ressourcen, optimieren die Kommunikation und helfen, Insellösungen von Anwendungen und Daten zu vermeiden. Je nach Unternehmens- und Organisationsgröße, Aufgaben, Organisationsformen und speziellen Unternehmensanforderungen sind die Vernetzungen, Komponenten und Administrationen sehr unterschiedlich dimensioniert. Externe Systemausstatter müssen daher mit ihren Kunden in detaillierte Gespräche eintreten und zusätzlich Ist-Analysen vor Ort durchführen, um Bedarfe und Anforderungen an eine zukunftsgerichtete Netzbereitstellung zu ermitteln. IT-Abteilungen müssen für die Bereitstellung ihrer Netzwerke ständig wichtige Leistungskennzahlen prüfen, um die Verfügbarkeit der Systeme und Anwendungen sowie Datensicherheit an allen Arbeitsplätzen zu gewährleisten. IT-Abteilungen und externe Systembetreuung müssen gut zusammenarbeiten, um die Anforderungen der Netznutzer zu erfüllen.

Netzwerke müssen aufgrund ihrer unterschiedlichen Dimensionen unterschiedliche Anforderungen erfüllen. So können nur wenige Clients in einem Kleinunternehmen im Netzwerk angeschlossen sein, das Netz aber höchste Sicherheitsanforderungen erfordern. In der Größe können Netzwerke für kleine und mittlere Unternehmen mehrere hundert Clients bedienen und in großen Unternehmenskonzernen mehrere zehntausend. Die im Netz laufenden Anwendungsprogramme und Dienste sind sehr unterschiedlich und müssen auf ihre Netzkompatibilität geprüft werden.

Benutzer der Clients müssen ihren IT-Abteilungen mitteilen, welche Anforderungen sie stellen. Kunden müssen externen Auftragnehmern ebenso spezifizieren, welche Leistungen zu erfüllen sind. Mitarbeiter der IT-Abteilungen müssen in der Lage sein, Fachkräfte anderer Abteilungen und ihre Arbeitsanforderungen zu verstehen und mit ihnen zu kommunizieren.



Für die Vertragsgestaltung bzw. die Vereinbarungen zwischen Auftraggeber und Auftragnehmer ist es wichtig, Vereinbarungen so klar zu formulieren, dass sie umsetzbar und auch kontrollierbar sind. Die Vereinbarungen müssen danach so umgesetzt, konfiguriert und bereitgestellt werden, dass die gestellten Anforderungen erfüllt werden.

TAG 1 und TAG 2 - Netzwerkbereitstellung nach unterschiedlichen Unternehmensanforderungen unterscheiden

Unternehmen mit mehreren Arbeitsplätzen setzen i.d.R. Netzwerke ein, um Systeme, Anwendungen und Daten vernetzt zu nutzen und über das Datennetz zu kommunizieren. Bevor konkrete Anforderungen zur Netzwerkbereitstellung nach unterschiedlichen Größen von Unternehmen und Netzwerken erarbeitet werden sollen, werden grundlegende Kompetenzen zur Bereitstellung entwickelt. Hierbei geht es zum einen darum, wie Kundenanforderungen formuliert werden sollen (z. B. als Lasten- oder Pflichten hefte). Zum anderen wird es in diesem Kapitel darum gehen, welche Methoden zur Zusammenarbeit häufig Anwendung finden. Inhaltlich werden Anforderungen grundlegend hinsichtlich ihrer technischen und sicherheitsrelevanten Spezifikationen erörtert, dazu werden auch wirtschaftliche Aspekte im Beschaffungs- und Bereitstellungsprozess betrachtet.

Für komplexe Beschaffungs- und Bereitstellungsmaßnahmen unter Beteiligung mehrerer Parteien (Auftraggeber und Auftragnehmer, Berater etc.) oder Personen werden i.d.R. Methoden des Projektmanagements oder agiler Projektmanagementmethoden angewendet. In der Grundstufe und in den anderen Lernfeldern der Fachstufe wurden Kompetenzen des Projektmanagements bereits entwickelt, sodass hierauf verwiesen wird. Diese sollten bei Bereitstellungsmaßnahmen einbezogen werden. Zum Projektmanagement in größeren Projekten siehe auch die vorherigen Module.

Projektmanagement - Kompetenzentwicklung in anderen Lernfeldern	
Grundstufe	1.5.2 Die Präsentation planen 2.5.3 Auftragsbearbeitung mit Projektmanagement unterstützen 5.3.2 Software im Rahmen eines Projektes entwickeln
Fachstufe	1.3.3 Lösungsbearbeitung in Teams 2.4.2 Projektplanung durchführen 3.1 Kundenaufträge in Software Projekten bearbeiten
Berufsstufe	Projektmanagement in größeren Projekten

LE 1 - Kundenanforderungen formulieren

Der grundsätzliche Prozess der Anforderungsanalyse wird im folgendem Schaubild beschrieben.

Prozess der Anforderungsanalyse



Die Bedarfs- und Anforderungsanalyse zur Netzbereitstellung ist weitaus komplexer, da die Netze der Betriebe und Organisationen sehr unterschiedlich in den Anforderungen, Größen und Anwendungsbereichen sind. Gerade in den letzten Jahren ergaben sich durch das Cloud-Computing ganz neue Möglichkeiten. Nicht selten müssen hybride (gemischte) Technologien berücksichtigt werden, dabei sollten die Risiken und Alternativen sorgfältig geprüft werden. Häufig ist die Unterstützung externer Berater mit Erfahrungskompetenzen notwendig. In der Ausbildung geht es darum, einen Einstieg in diese komplexen und vielfältigen Bereitstellungs Herausforderungen zu erhalten und an Bereitstellungsprojekten mitarbeiten zu können.

LE 2 - Einsatzgebiete

Nach der Ausbildungsordnung der IT-Berufe werden jedem Ausbildungsberuf bestimmte Einsatzbereiche zugeordnet, in dem besonders ausgebildet werden soll. Die folgende Tabelle gibt Einsatzgebiete an, die einen besonderen Bezug zur Auswahl und Bereitstellung von Netzen haben.

Einsatzgebiete in der Bereitstellung von Netzen und Diensten nach den Ausbildungsordnungen		
Einsatzgebiete	Aufgaben	
Rechenzentren	Aufbau, Erweiterung und Betrieb von Rechenzentren, Aufrüsten von Komponenten, Herstellen und Erweitern/Ändern der Verkabelung, Administration, Monitoring etc.	
Digitale Infrastrukturen	Netze der Informations- und Telekommunikationstechnik betreiben (Kupfer-, Glasfaser- und drahtlose Netze), passive und aktive Komponenten bereitstellen	
Netzwerke	Netzwerke logisch und physisch einrichten, passende Geräte auswählen und konfigurieren etc.	
	Festnetze	Kupfer-, Glasfaser-Verkabelung herstellen, ändern, prüfen
	Funknetze	Funkzellen einrichten und betreiben
Virtuelle Netze	virtuelle Netze auf physischen Netzen betreiben (VLAN, VPN) und Netze in virtualisierten Strukturen (IaaS) anbieten	
Sicherheitssysteme	Sicherheit von Netzen herstellen durch Firewall, Demilitarized Zone (DMZ), Intrusion Detection Systeme (IDS), Zugriffskonzepte (Berechtigungssysteme) etc.	
Technische IT-Services	Dienste der Informationstechnik bereitstellen, Tests und Wartungen durchführen	
IT-System-Betreuungen	IT-Systeme warten und betreiben	

LE 3 - Betriebsmodelle

Als Betriebsmodelle für die Bereitstellung von Netzen und Diensten lassen sich unabhängig von der Größe und Vielfalt vereinfacht das lokale bzw. klassische Netzwerk (LAN) vom Cloud-Computing und hybriden Modellen (gemischten Systemen) unterscheiden. Die Entscheidung für oder gegen ein Betriebsmodell ist grundlegend und damit von großer Bedeutung für den Erfolg, den Aufwand und die Kosten der Netzbereitstellung. Dazu kommen Aufwandsbetrachtungen (Kosten, Zeitaufwand, Fachkräfteeinsatz) in der Umstellung und den laufenden Betrieb.

Betriebsmodelle in der IT-Vernetzung	
Lokale/klassische Vernetzung (LAN)	Die benötigten Dienste werden lokal mit eigenen Servern im eigenen Netz zur Verfügung gestellt. Dies bedingt, dass Hardware bereitgestellt, Software installiert und das gesamte System verwaltet und gewartet werden muss.
Cloud Computing (virtuelle Vernetzung)	Die benötigten Dienste werden in der Cloud umgesetzt. Netzwerke und Dienste werden Virtualisiert. Der Zugriff erfolgt über einen Browser.
Gemischte/hybride Vernetzung (LAN-Cloud)	Ein Teil der Dienste wird beispielsweise als private Cloud in einem gesicherten Bereich bereitgestellt, ein anderer als Public Cloud einem größeren Nutzerbereich.

LE 4 - Erstgespräche mit Kunden

Jeder neuen Bereitstellung geht eine Ist-Analyse des vorhandenen Systems, der Rahmenbedingungen und der Wünsche des Kunden voraus. Da die Netzbereitstellung alternativ auch mit völlig unterschiedlichen Systemen und Diensten erfolgen kann, sind im Bereitstellungsprozess die Ziele des Kunden festzustellen. Es kann im einfachsten Fall sein, dass keine Erweiterung oder Migration des Netzwerkes nötig ist, sondern einfach die Verfügbarkeit des Netzes durch eine Leistungssteigerung bzw. Skalierung verbessert wird.

Die Feststellung der Kundenanforderungen kann in drei Phasen verlaufen. Während im ersten Kundengespräch Informationen zum Netzsystem eingeholt sowie Probleme und Wünsche des Kunden erörtert werden, werden im Lastenheft vom Kunden schon konkret Festlegungen vorgenommen, was der Kunde bereitgestellt haben möchte und wofür diese Bereitstellung dient. Auch werden hierbei die Ziele und Rahmenbedingungen beschrieben.

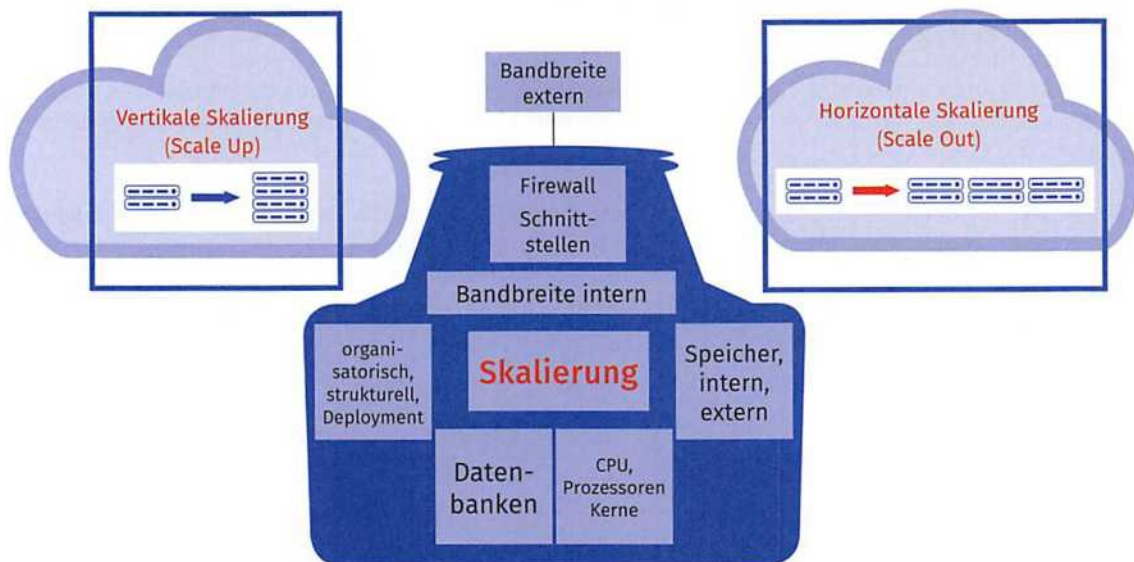


Der Auftragnehmer wird aus dem Lastenheft die fachliche Konzeptionierung vornehmen und ein Pflichtenheft erstellen. Das Pflichtenheft dient wieder als Grundlage für Ausschreibungen oder die Bereitstellung der Netzanforderungen durch den Auftragnehmer.

Da es sich bei großen Netzbereitstellungen um sehr komplexe und auch finanziell teure Anschaffungen handelt, werden im Projektmanagement auch besondere Managementsysteme eingesetzt. Diese helfen, Beschaffungs- und Bereitstellungsprozesse zu unterstützen und möglichst reibungslos durchzuführen. Bevor Neuanschaffungen, Erweiterungen oder sogar eine Migration auf ein anderes System durchgeführt werden, muss geprüft werden, ob und wie lange das System durch eine bessere Skalierung seine Aufgaben erfüllen kann. Beklagt der Kunde Performance-Probleme, so wird häufig nach dem Engpass- oder Flaschenhalsbereich gesucht.

Bei einer horizontalen Skalierbarkeit wird die Leistung oder Verfügbarkeit der Ressource erhöht, indem mehrere Hardware- oder Softwarekomponenten miteinander zu einer einzigen logischen Einheit verbunden. Bei der vertikalen Skalierbarkeit dagegen wird die Leistung oder Verfügbarkeit durch Aufrüsten durch mehr Ressourcen (z. B. RAM, CPU) zu einem Server erreicht. Die horizontale Skalierbarkeit hat den Vorteil, die Kapazitäten im laufenden Betrieb und theoretisch grenzenlos zu erhöhen. In der vertikalen Skalierbarkeit bestehen Beschränkungen durch die vorhandene Hardware. Zudem erfordert das sogenannte Scaling Up i.d.R. eine Ausfallzeit.

Bei virtuellen Systemen verschiebt man einfach im laufenden Betrieb die virtuellen Maschinen auf performantere Hardware und löst so ganz einfach ein Skalierungsproblem.



Eine geringere Performance im Netzwerk kann darüber hinaus vielfältige Gründe haben, die auch in organisatorischen und strukturellen Verbesserungspotenzialen, in notwendigen Upgrades oder Schnittstellen begründet sein können.

Ziele und Migrationsstrategien der Netzbereitstellung

Skalierung

Fähigkeit eines Systems, Netzwerks oder Prozesses zur Leistungsveränderung. Dabei müssen Ressourcen wie CPU, RAM, Festplatten, Bandbreite angepasst werden, Software- und Treiberupdates durchgeführt werden. In Cloudsystemen geschieht dies einfach und schnell durch Provisionierung höherer Ressourcen.

- Vertikale Skalierung: Aufrüsten zu bestehenden Einheiten
- Horizontale Skalierung: Hinzufügen von Ressourcen zu einer logischen Einheit durch zusätzliche physische Einheiten mit Vorteilen: theoretisch unbegrenzt im laufenden Betrieb

Testinstallation, Neuinstallation, Erweiterung, Ersatz

Zunächst ist zu klären, wie umfangreich die Netzbereitstellung ist. Es bietet sich zur sicheren Umstellung auf ein neues System eine Testinstallation an. Auch muss geprüft werden, wie die Umstellung zu erfolgen hat: Direkt-, Stufen-, Parallel- oder Probееinführung.

Migration

In der IT wird mit Migration (lat. *migratio*: Wanderung, Übersiedlung) der Prozess einer grundlegenden Veränderung einer bestehenden Systemlandschaft oder eines wesentlichen Teils verstanden und kann unterschiedliche Ausrichtungen haben:

- **Hardware-Migration:** z. B. der Wechsel auf eine neue Servergeneration mit anderen Prozessoren etc. oder der Wechsel vom klassischen Ethernet-Netzwerk zur ATM-Technologie unter Beibehaltung der vorhandenen strukturierten Verkabelung
- **Software-Migration:** geht über eine einfache Aktualisierung/ein Upgrade hinaus und beschreibt einen grundlegenden Wechsel der Software-Infrastruktur
- **Live-Migration:** Wechsel auf ein anderes System im laufenden Betrieb, z. B. Umzug einer virtuellen Maschine (VM), von einem physikalischen Wirtssystem (Host) auf ein anderes System, z. B. aufgrund von Umstellungen auf neuere Schnittstellen, Techniken oder Versionen
- **On-Premises-to-Cloud-Migration:** Wechsel von einem Anwendungssystem mit Datenhaltung lokal auf eigenem Server bei eigener Administration im Unternehmen zu einem Cloudserver mit Diensten eines Providers und Datenhaltung in der Cloud sowie externer Administration je nach Dienst.

Für die Befragung der Kunden ist eine Checkliste oder ein Leitfaden hilfreich. Auch sollten Protokolle über die Ergebnisse der Erstgespräche erstellt werden, damit es später keine Missverständnisse über die Ergebnisse der Gespräche gibt und die Zuständigkeiten bzw. weiteren Zuarbeiten vereinbart und schriftlich festgehalten werden.

Erstgespräch zur Analyse von „Netzwerken & Diensten“	
Kategorien	Befragungen im Kundengespräch
Arbeitsplätze (Clients)	Ist-Zustand: Angabe der Anzahl von vernetzten internen und externen Arbeitsplätzen, wie stark diese das Netzwerk beanspruchen, wie groß für die Arbeitsplätze die Arbeitseinschränkung durch zeitweisen Netzwerkausfall ist, welche Sicherheitsforderungen (Datensicherheit, Backup, Datenschutz) speziell zu berücksichtigen sind etc. Soll-Zustand: Ändern sich Anzahl Clients oder die Vernetzung zu Arbeitsplätzen (z. B. zu Homeoffice, mobile Offices) bzw. ändern sich Anforderungen, welche Störungen oder Unzulänglichkeiten sollen über Vernetzung behoben werden?
Betriebssystem, Anwendungsprogramme	Ist-Zustand: Welches Betriebssystem ist derzeit installiert und welche Anwendungsprogramme mit Angabe der Version und Lizenzierung? Soll-Zustand: Kundenwünsche, z.B. Migration auf Cloud-Dienste unter Nennung der wichtigen Anwendungsfälle?
Vernetzte Peripheriesysteme	Ist-Zustand: Es ist zu klären, welche Peripheriegeräte über das Netz erreichbar sind und auch genutzt werden (z.B. Drucker, DMS, Back-up-Systeme, Kameras). Soll-Zustand: Welche Geräte sollen anders oder zusätzlich im Netz genutzt werden?
Netzwerkssystem	Ist-Zustand: Welche aktiven und passiven Netzwerkkomponenten werden eingesetzt, welche sind unterdimensioniert oder stören den Netzbetrieb, wo fehlen Netzwerkanschlüsse bzw. Vernetzungen? Soll-Zustand: Wo sehen Kunden Verbesserungspotenziale, z. B. durch zusätzliche Installation von Access Points, Repeatern?
Datensicherung	Ist-Zustand: Wie wird die Datensicherheit gewährleistet, z. B. durch welche Firewall, Sicherheitsprogramme, Back-up-Systeme? Soll-Zustand: Welcher erhöhte Sicherheitsstandard wird gefordert?

Erstgespräch zur Analyse von „Netzwerken & Diensten“	
Kategorien	Befragungen im Kundengespräch
Administration und Support	Ist-Zustand: Wer verwaltet derzeit das Netzwerk, wer leistet Support und worin bestand dieser in der letzten Zeit? Waren Administration und Support ständig bzw. zur vollsten Zufriedenheit verfügbar? Was kostete der Support? Soll-Zustand: Gibt es Änderungswünsche aus Kundensicht bzw. Änderungsbedarf aus Beratersicht?
Sicherheitsanforderungen	Ist-Zustand: Welche Sicherheitssysteme und -programme werden eingesetzt, welche Störungen gab es in der Vergangenheit, welche Neuerungen werden im Markt angeboten? Liegt eine Schutzbedarfsanalyse vor? Soll-Zustand: Welche Sicherheitsanforderungen sollen gewährleistet werden?
Besondere Zielsetzungen	Kostenoptimierung: Sind aus Kundensicht die Kosten zu hoch? Zukunftsorientierung: Gibt es Entwicklungen in der Netzwerktechnik, die dringend bzw. aus Kundensicht umgesetzt werden sollen? Administrationsänderungen: Sollen Änderungen in der Netzwerkadministration geprüft werden? Compliance-Anforderungen: Bestehen erhöhte rechtliche Anforderungen oder Anforderungen durch Unternehmensrichtlinien, die berücksichtigt werden sollen? Sicherheitsanforderungen: Ist eine Schutzbedarfsanalyse notwendig bzw. durchgeführt und gibt es höhere Sicherheitsanforderungen? Sonstige: Welche sonstigen Anforderungen werden aus Kundensicht geäußert?

LE 5 - Lastenhefterstellung

Im weiteren Verlauf sollen aufbauend auf dem Erstgespräch mit den Kunden Lastenhefte unterschiedlicher Kunden besprochen bzw. bearbeitet werden (siehe auch bereits erarbeitete Kompetenzen dazu und die Bereitstellung von Netzen).

Lastenheft - User Requirement Specifications

Laut DIN 69901-5: 2009-01 (Begriff 3.32) ist das Lastenheft die vom Auftraggeber festgelegte Gesamtheit der Forderungen an die Lieferungen und Leistungen eines Auftragnehmers innerhalb eines (Projekt-)Auftrags. Alternativ werden Begriffe wie beispielsweise Anforderungskatalog, Kundenspezifikation oder Leistungsverzeichnis verwendet.

Das Lastenheft - was und wofür

Wenn möglich sollten hier noch keine technischen Lösungen (fest) vorgegeben werden, um optimale technische Lösungen nicht einzuschränken. Zu beachten ist:

- Das Lastenheft wird grundsätzlich (i.d.R.) vom Auftraggeber erstellt.
- Es wird auch als Leistungsverzeichnis (LV) des Kunden bezeichnet.
- Das Lastenheft beschreibt auch Rahmenbedingungen der Leistungserbringung (z. B. Normen, Richtlinien, Standards, Eigenleistungen), vom Kunden gewünschte vertragliche Konditionen (z. B. Gewährleistungsanforderungen, Vertragsstrafen, Risikomanagement), Anforderungen an den Auftragnehmer (z. B. notwendige Referenzen und Zertifizierungen).
- Planer (z. B. IT-Abteilung des Kunden oder externe Berater) unterstützen den Auftraggeber in der Entwurfsphase bei der Erstellung des Lastenheftes.

- Das Lastenheft dient als Grundlage für die Erstellung des Pflichtenheftes oder für eine RFI (Request for Information, allgemeine Anfrage).
- Die Erstellung von Lasten- und Pflichtenheften erfolgt i.d.R. in Projekten. Einige wichtige Begriffe zum Projektmanagement werden daher folgend in Erinnerung gerufen, mehr wird im Arbeitsbuch zur Bearbeitung herausgestellt.

Projektmanagement - Begriffe aus der DIN 69901-5:2009-01

Begriffe für das Gespräch mit Kunden

Abnahme: unternehmerische Entscheidung des Auftraggebers, dass ein (Teil-)Ergebnis den Vereinbarungen und Erwartungen entspricht und somit als Grundlage für nachfolgende Prozesse verwendet werden kann und muss (Begriff 3.3)

Anforderung: Beschaffenheit, Fähigkeit oder Leistung, die ein Produkt, Prozess oder die am Prozess beteiligte Person erfüllen oder besitzen muss, um einen Vertrag, eine Norm, eine Spezifikation oder andere, formell gegebene Dokumente zu erfüllen (Begriff 3.7)

Aufwandsschätzung: einmalige oder wiederholte Schätzung von Kosten-, Zeit- und/oder Ressourcenbedarf, insbesondere für zukünftige Vorgänge, Arbeitspakete oder Projekte (Begriff 3.12)

Projektstrukturplan: vollständige, hierarchische Darstellung aller Elemente (Teilprojekte, Arbeitspakete) der Projektstruktur als Diagramm oder Liste (Begriff 3.82)

Ressource: abgrenzbare Gattung bzw. Einheit von Personal, Finanzmitteln, Sachmitteln, Informationen, Naturgegebenheiten, Hilfs- und Unterstützungsmöglichkeiten, die zur Durchführung oder Förderung von Vorgängen, Arbeitspaketen oder Projekten herangezogen werden können (Begriff 3.91)

Risikoanalyse: Projektmanagementprozess, der die Identifikation und Bewertung von Projektrisiken umfasst (Begriff 3.95)

Stakeholder-Analyse: Analyse der Projektbeteiligten hinsichtlich deren Einfluss auf das Projekt und deren Einstellung (positiv oder negativ) zum Projekt (Begriff 102)

Zieldefinition: quantitative und qualitative Festlegung des Projektinhaltes und der einzuhaltenden Realisierungsbedingungen, z.B. Kosten und Dauer oder Muss- und Kann-Ziele (Begriff 3.109)

Sonstige Hinweise

Ziele: Sie sollten S-M-A-R-T (spezifisch, messbar, ausführbar, realistisch, terminiert) formuliert werden.

Meilensteine: Nach DIN 69900 ist ein Meilenstein ein „Ereignis besonderer Bedeutung“, z.B. Teilprojektabschluss oder Zwischenergebnis, Termin für wichtige Teambesprechung oder richtungsweisende Entscheidungen im Projekt.

Funktionale Anforderungen: Sie beschreiben allgemein die Fähigkeiten eines Systems, die ein Anwender erwartet, um mithilfe des Systems ein fachliches Problem zu lösen. Die Anforderungen werden bezogen auf das Netzwerk aus den zu unterstützenden Vernetzungen und die Inanspruchnahme abgeleitet.

Nicht funktionale Anforderungen: Hier werden Anforderungen an das System beschrieben, die nicht-fachlicher Natur sind, jedoch entscheidend zur Anwendbarkeit des Systems beitragen, beispielsweise Qualitätsanforderungen, Compliance, Nachhaltigkeitsanforderungen, Sicherheitsanforderungen oder Benutzer-/Administrationsanforderungen.

IT-Sicherheitsanforderungen und Schutzbedarf: Aufgrund der besonderen Sicherheitsanforderungen von IT-Systemen werde diese häufig nicht unter den nicht funktionalen Anforderungen aufgeführt, sondern gesondert herausgestellt. Hierbei sind Sicherheitsrichtlinien und Anforderungen aus der Schutzbedarfsanalyse zu benennen, die die Vertraulichkeit, Integrität und Verfügbarkeit des Systems gewährleisten.

Bezogen auf die Gliederungen zum Lastenheft soll folgende Ausbildungsvorlage helfen, konkrete Anforderungen für das Bereitstellen von Netzen zu diskutieren und zu erarbeiten.

**Inhalte Lastenheft „Bereitstellung von Netzwerken und Diensten“
(Ausbildungsvorlage)**

1. Ausgangssituation analysieren und Zielsetzung

- 1.1. Ausgangssituation: Hier werden bestehende Anwendungen und Prozesse im Betriebsablauf und vorhandene Systeme beschrieben.
- 1.2. Zielsetzung: Hier wird der gewünschte Sollzustand an Netzwerken und Diensten sowie ihrer KPI (Schlüsselkennzahlen) aus Kundensicht beschrieben.

2. Funktionale Anforderungen

- 2.1. Muss-Kriterien: Welche betrieblichen Anwendungen und Prozesse müssen vom System unterstützt werden und im Netz zu welchen Zeiten verfügbar sein, welche Muss-Kriterien an die Administration gestellt sein?
- 2.2. Kann-Kriterien: Welche weiteren funktionalen Anforderungen oder Ausbaustufen sind relevant?
- 2.3. Abgrenzungskriterien: Welche Kriterien bzw. Fälle sollen bzw. dürfen nicht eintreten?

3. Nicht funktionale Anforderungen

Folgende Fragestellungen zur Netzbereitstellung können genannt werden:

- 3.1. Qualität: Welche Qualitätsanforderungen werden an die Netzwerktechnik gestellt?
- 3.2. Administration: Welche Anforderungen werden an die Administrierung und Orchestrierung gestellt?
- 3.3. Spezielle Anforderungen: Werden besondere Anforderungen bzgl. Compliance oder Nachhaltigkeit gestellt? Welche Anforderungen werden bzgl. des Berechtigungssystems (Zugriffsberechtigung) gestellt, ist die Einhaltung von Standards und Gesetzen zu beachten?

4. Sicherheit und Datenschutz

Sicherheit und Datenschutz als nicht funktionale Anforderungen werden häufig wegen der großen Bedeutung gesondert herausgestellt und Bezug auf die BSI-Schutzbedarfsanalyse und Risikoanalysen genommen.

- 4.1. Allgemeine Anforderungen: Datensicherung und TOM aus Kundensicht werden genannt etc.
- 4.2. Besondere Anforderungen: Verschlüsselung von E-Mails, VPN, Website-Schutz, Firewall etc.

5. Lebenszyklus des Netzwerksystems: Die Anforderungsanalyse umfasst neben der erstmaligen Bereitstellung den fortlaufenden Betrieb, Wartungsaufgaben, Vorgaben zur Erstellung von SLA.

- 5.1. Zeitpunkt und Zeitraum der Umsetzung: Beginn und Ende des Bereitstellungsprojekts, Wartungsregelungen
- 5.2. Abzulösende Systeme: Welche Systeme werden außer Betrieb genommen?
- 5.3. Wartung und Administration: Kundenvorgaben, die in SLA aufgenommen werden sollen

6. Lieferumfang: Zeit, Umfang, Kommunikation, Abnahmekriterien und Abnahmemaßnahmen

- 6.1. Infrastruktur: Welche Infrastruktur zur Netzbereitstellung liegt vor und welche muss neu bereitgestellt werden, liegt ein aus Kundensicht erstellter vereinfachter Vernetzungsplan vor (Ist/ Soll), welcher Erweiterungsbedarf wird sich in der Zukunft ergeben?
- 6.2. Netzbereitstellung: Welche Anwendungen werden angefordert? Sind Software-Lizenzen auszuliefern? Welche Anwendungen müssen implementiert und konfiguriert werden?
- 6.3. Dokumentation, Abnahme, Einweisung und Schulung: Welche Kundenanforderungen werden gestellt?

Als Ausbildungsvorlage wurde bei JIKU IT-Solutions folgende Anforderungsvorlage zum Lastenheft entwickelt. Sie wird den neuen Auszubildenden als Diskussionsvorlage und zur Erstellung von Alternativen ausgehändigt.

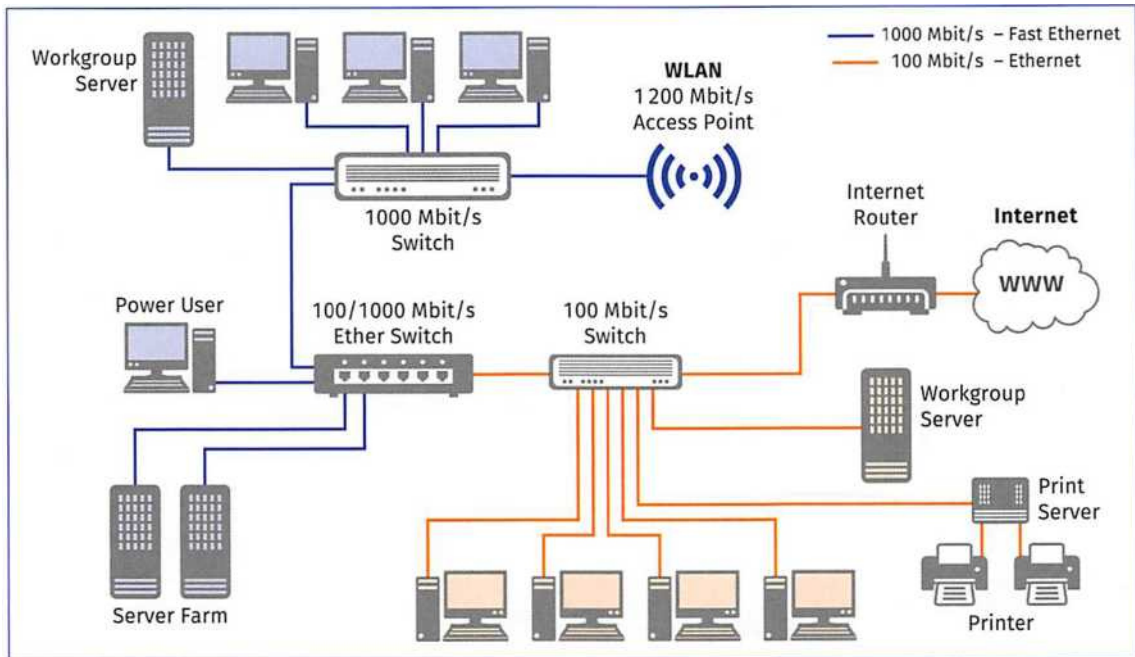
Vorlage für die Anforderungsanalyse		JIKU IT-Solutions	
Kundenanforderungen			
Lastenheft Netzwerkbereitstellung (Ausbildungsversion)			
Kriterien	Bewertungs- und Beratungshinweise für das Kundengespräch		
Zielgruppen	☐ interne Nutzer ☐ externe Nutzer/ Niederlassungen ☐ weitere _____		
Anzahl Anwender	intern []	extern []	weitere []
Bereitstellung für Nutzung	☐ Einfache Nutzung ☐ Parallele Nutzung	max. _____ parallele Anfragen pro _____	max. Verzögerung pro Anfrage geduldet: _____
Zugriffsort/Clients	☐ lokal, z. B. aus Büro ☐ mobil, _____ ☐ externe Nutzer, Internet		
Verfügbarkeit	☐ ständig, 24/7 ☐ andere _____		
Schnittstellen			
Schnittstellen extern	☐ EDI ☐ DATEV ☐ sonstige _____		
Hardware & Software			
Hardware	☐ Server vorhanden ☐ Spezialhardware im Einsatz _____		
Software – Anwendungstypen	☐ E-Mail ☐ Webseite ☐ Shop _____ ☐ Fernzugriffe _____ ☐ Groupware _____ ☐ ERP _____ ☐ andere: _____		
Netzwerk			
LAN-Verkabelung	☐ strukturierte Verkabelung vorhanden	☐ WLAN vorhanden Anzahl Access-Points: _____	☐ Direktanschluss
WAN-Anschluss	☐ DSL ☐ Kabel-TV ☐ LWL ☐ Mobilfunk		
Betrieb & Administration			
Administration	☐ intern ☐ extern _____ ☐ andere: _____		
Bei externer Administration, SLA-Basisvertrag			
Verfügbarkeit	☐ sehr hoch ☐ hoch ☐ Sonstiges: _____		
Informationssicherheit			
Datenübertragung extern	☐ Externe Datenhaltung ☐ Telefonie ☐ Fernzugriff		
Maximale Ausfallzeit	☐ < 2 Stunden ☐ < 1 Arbeitstag ☐ sonstige _____		
Anforderungen	Datenschutz: _____ Datensicherheit: _____ sonstige: _____		
Backup-Sicherung	☐ gewöhnlich ☐ wichtig ☐ Sonstiges: _____		
Support und Ergänzungen			
Support & Wartung	☐ Support bisher: _____ Sonstiges: _____		

LE 6 - Pflichtenhefterstellung

Auf der Basis des vom Kunden bereitgestellten bzw. unterzeichneten Lastenheftes wird i.d.R. vom Auftragnehmer der Netzbereitstellung ein Pflichtenheft erstellt. Dieses Pflichtenheft gibt fachlich konkret an, wie der Auftragnehmer die Anforderungen des Lastenheftes umsetzen bzw. realisieren will.

Ein Problem ist für den Auftragnehmer, dass Kunden die vor der Vertragsunterzeichnung gegebenen konkreten Pflichtenhefte verwenden könnten, um Konkurrenzangebote einzuholen und dann den Mitbewerber mit der Bereitstellung zu beauftragen. Daher geben Unternehmen dem Kunden die genauen Kalkulationsangaben i.d.R. nicht preis, sondern nur die für die vertragliche Festlegung notwendigen Informationen und Gesamtpreise. Für die interne Kalkulation und Arbeitsvorbereitung müssen jedoch genaue fachliche Vorgaben an Komponenten, Material und Arbeitsstunden in Menge und Qualität sowie Selbstkosten ermittelt werden.

Dem Lastenheft kann vereinfacht und dem Pflichtenheft fachlich spezifiziert ein Vernetzungsplan beigelegt werden.



Vernetzungsplan

Pflichtenheft - Fachkonzept (Functional Specifications)

Laut DIN 69901-5: 2009-01 vom Auftragnehmer erarbeitete Realisierungsvorgaben auf der Basis des vom Auftraggeber vorgegebenen Lastenheftes (Begriff 3.40). Auch in VDI-Richtlinien, z. B. 2519 oder 3694, werden Angaben im Pflichtenheft als Beschreibung der Realisierung aller Kundenanforderungen, die im Lastenheft gefordert werden, festgelegt. Anstelle eines Pflichtenheftes werden in der Praxis auch die Begriffe Fachspezifikation, Fachfeinkonzept, Sollkonzept, funktionale Spezifikation, Gesamtsystemspezifikation, Systemspezifikation u.a. verwendet.

Das Pflichtenheft - wie und womit

Zu beachten sind:

- Das Pflichtenheft bildet die Grundlage der vertraglich festgehaltenen Leistungen eines Auftragnehmers.
- Es beschreibt die Art der Umsetzung des vom Auftraggeber vorgegebenen Lastenheftes durch den Auftragnehmer.
- Das Pflichtenheft wird allgemein im Rahmen der Werk- und Montageplanung des Auftragnehmers aufgestellt.
- Im Pflichtenheft sind Infrastruktur, Vernetzung, Verkabelung, Komponenten, Protokolle, Anwendungen, Anforderungen, Dienste fachlich so genau spezifiziert, begründet und überprüfbar wie möglich festzulegen.
- Der Auftragnehmer ist nicht verpflichtet, im Pflichtenheft genaue Kalkulationsgrundlagen für die Preiskalkulation offenzulegen.

- Ersteller sollten missverständliche Aussagen vermeiden, um den Projekterfolg nicht durch Differenzen zu gefährden. Eindeutige Aussagen, KPI oder „S-M-A-R-Te“ Ziele sind zu formulieren.
- Mindestbestandteile sollten Projektstrukturplan mit den Arbeitspaketen, den fachlichen Anforderungen und den Rahmenbedingungen sein.
- Um komplexe Inhalte verständlich zu vermitteln, bieten sich grafische und strukturierte Darstellungen (z.B. Netzpläne, Diagramme, Tabellen oder Mindmaps) an.
- Das Pflichtenheft sollte immer von Auftraggeber und Auftragnehmer unterzeichnet werden, als Vertragsbestandteil, z.B. im Liefer- oder Werkvertrag bzw. in den SLA festgelegt werden, die Umsetzung erst nach Unterzeichnung und Auftragserteilung beginnen.

Eine Gliederung ist gesetzlich nicht vorgeschrieben und auch abhängig von Umfang und Art der Bereitstellung. Entsprechend den Gliederungsvorschlägen wurde bei JIKU IT-Solutions folgende Ausbildungsvorlage für die Netzbereitstellung erarbeitet und zur Diskussion gestellt.

Inhalte Pflichtenheft „Bereitstellung Netzwerke und Dienste“ (Ausbildungsvorlage)

- 1. Ausgangssituation analysieren und Zielsetzung**
 - 1.1. Ausgangssituation: genaue technische Beschreibung entsprechend dem Lastenheft und der Ist-Analyse.
 - 1.2. Zielsetzung: fachliche Beschreibung der Zielsetzung, Teilziele (S-M-A-R-T) und Unternehmensrichtlinien
 - 1.3. Sollkonzept: fachliche Angaben wie Netzplan, Schnittstellen, KPI, Verweise auf die folgenden Unterpunkte
- 2. Funktionale Anforderungen**
 - 2.1. Muss-Kriterien: Leistungsgrößen und KPI von Infrastruktur, Netzkomponenten und Netzdienste/-Software
 - 2.2. Kann-Kriterien: Erweiterungsmöglichkeiten, Upgrade-Regelungen, Alternativen, mögliche Unterstützungen
 - 2.3. Abgrenzungskriterien: insbesondere Nennung erhöhter Leistungsgrößen, die nicht relevant sind
- 3. Nicht funktionale Anforderungen**
 - 3.1. Qualität: Qualitätsmerkmale der Netzbereitstellung (Infrastruktur, Komponenten, Dienste)
 - 3.2. Administration: Angaben entsprechend den SLA, für interne und externe Administration, Monitoring, Wartung
 - 3.3. Spezielle Anforderungen: entsprechend den Unternehmensvorgaben konkrete Vorgaben
- 4. Sicherheit und Datenschutz:** entsprechend Schutzbedarfsanalysen, Risikoanalysen, DSGVO; DSG und anderen zu beachtenden Richtlinien festlegen
 - 4.1. Allgemeine Anforderungen: konkrete Nennung von TOM, Datensicherungsanforderungen und zu gewährende Sicherheitsstufen
 - 4.2. Besondere Anforderungen: entsprechend dem Lastenheft werden fachliche Vorgaben erstellt
- 5. Lebenszyklus des Netzwerksystems:** Es wird genau angegeben, welche Nutzungszeiten die Komponenten haben, welcher Ersatz und welche Wartung einzuplanen sind.
 - 5.1. Zeitpunkt und Zeitraum der Umsetzung: genaue zeitliche Projektplanung
 - 5.2. Abzulösende Systeme: z.B. durch tabellarische Übersicht und Netzplan (Ist/Soll)
 - 5.3. Wartung und Administration: Festlegung, wer, was, wie, mit welchen Ressourcen, wann und wie überprüfbar erledigt

6. Lieferumfang: Wie und wann erfolgt die Lieferung?

5.4. Infrastruktur: fachliche Vorgaben der notwendigen Infrastruktur (vorhanden und bereitzustellen)

5.5. Netzwerkbereitstellung: fachliche Vorgaben für aktive und passive Komponenten, Dienste etc.

5.6. Dokumentation, Abnahme, Einweisung und Schulung: genaue fachliche Vorgaben

Entsprechend den Forderungen der Ausbildungsordnungen und Prüfungskatalogen wurde in einer JIKU- Ausbildungssitzung folgende Zusammenstellung von Stichworten gesammelt und zur Diskussion gestellt. Diese Zusammenstellung von Fachbegriffen der Komponenten und Spezifikationen soll möglichst bei der Pflichtenheftformulierung berücksichtigt werden.

Stichwortsammlung zur Konzeption der Netzwerkbereitstellung im Pflichtenheft (Zusammenstellung in einer JIKU-Ausbildungssitzung)

Virtualisierung, Bare Metal, verwendete und zu verwendende Infrastruktur (z. B. eigene Server + Storage, Cloud Computing), Ausdehnung, (LAN/WAN/MAN/GAN), Sicherheitskonzepte und -risiken, Übertragungswege, strukturierte Verkabelung (Funk, Kupferkabel, Glasfaser), Topologien, Einsatz Peer-2-Peer bzw. Client-Server-Konzepte, Datenübertragungsrate, Verschlüsselung (Preshared Key, RADIUS etc.), VLAN, drahtlos PAN/WLAN, Bluetooth, Einsatz Netzwerkprotokolle (IPv4/IPv6, TCP/UDP, SSL/TLS (Version), Schicht-5-7-Protokolle (z. B. DNS, IMAP, SMTP, HTTPS, SFTP, SSH), Übertragungsprotokolle (TCP/UDP, HTTPS), Speicher-Netzwerkprotokolle (iSCSI, Fibre Channel, FCoE, NFS, SMB/CIFS, HTTP und NVMe-oF), standortübergreifende und -unabhängige Kommunikation (VPN-Modelle, Tunneling, IPsec)

Anforderungen Systemkomponenten (Server, Peripheriegeräte, Clients, Storage, Appliance, Virtualisierung, Betriebssysteme, Anwendungen, Sicherheitsaspekte etc.), WAN-Modem (DSL-Modem), Router, Switches, WLAN-Controller, Access Point, Firewall, Loadbalancer, Managed Services

Anforderungen Netzwerk (z. B. Bandbreite, Latenz, Verfügbarkeit, Übertragungsmedium, Netzwerksicherheit), Funktions- und Belastungstest (z.B. Redundanz/Load Balancing/Mesh), netzwerkrelevante Dienste (DNS, DHCP, Proxy, Spanning Tree, dynamisches/statisches Routing, VLAN, First Hop Redundancy, QoS etc.), Anwendungsdienste (z. B. Echtzeitkommunikation, Mail-Server, Webserver, Groupware, Datenbanken), Service- und Liefermodelle (Cloud Computing und Fog Computing, IaaS, PaaS, SaaS, XaaS etc.)

Protokolldateien/Monitoring und Dokumentation (z. B. Ping, Trace Route, Analyse-Tools, z. B. Pakettracer, Wireshark, Netzwerkmonitoring, z. B. SNMP), Schutzziele bzw. Grundwerte der Informationssicherheit (Vertraulichkeit, Authentizität/Integrität, Verfügbarkeit), Festlegung der Schutzbedarfskategorien (normal, hoch, sehr hoch), Ergebnisse der Schutzbedarfsanalyse und Risikoanalyse, Zusammenarbeit mit Sicherheitsbeauftragten, Abstimmung mit ITSM, Beachtung der BSI-Grund- Schutzbausteine zur Vernetzung

Technische organisatorische Maßnahmen (TOM): Risiken identifizieren, Maßnahmen planen und Ausfallwahrscheinlichkeiten bestimmen, Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS), Sicherstellung des Betriebes elektrotechnisch (USV), hardwaretechnisch (redundante Systeme, RAID), softwaretechnisch (Back-ups), Zutrittskontrolle (z. B. Alarmanlage, Videoüberwachung, Besucherausweise), Zugangskontrolle (z. B. zum Gebäude, Serverraum, Schrank, Bildschirmschoner mit Passwortschutz, biometrische Verfahren, Magnet- oder Chipkarte), Zugriffskontrolle z. B. durch Verschlüsselung von Datenträgern, Löschung von Datenträgern, User-Management/Rollenkonzept, Firewall/Webfilter, Portsecurity, Log Management, Compliance Reports, Berechtigungskonzepte, Organisationsstrukturen (Zugang, Zutritt, Zugriff)

Berücksichtigung der 3-2-1-Regel für Backups:

- Drei Kopien aller kritischen Daten sollten mindestens auf
- zwei unterschiedlichen Medien existieren,
- ein Medium davon sollte außerhalb/extern gelagert werden.

Zur Risikoreduzierung und -vermeidung sind insbesondere auch Festlegungen zur Redundanz bzw. zur Bereitstellung redundanter Systeme zu treffen.

Einsatz redundanter Systeme (Redundanz)

Redundanz (lat. *redundare*: überlaufen, reichlich ergießen) bedeutet das zusätzliche Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems, auch wenn diese bei einem störungsfreien Betrieb im Normalfall nicht benötigt werden.

Funktionelle Redundanz: Sicherheitstechnische Systeme werden mehrfach parallel ausgelegt, damit beim Ausfall einer Komponente die anderen die geforderten Dienste gewährleisten können.

Redundante Datensicherung: Datensicherung nach Erfordernis redundant (mehrfach parallel).

Räumliche Redundanz: Zusätzlich versucht man, die redundanten Systeme voneinander räumlich zu trennen, um Risiken durch Störungen vor Ort zu minimieren.

Organisatorisch diversitäre Redundanz: Es wird organisatorisch darauf geachtet, dass Störungen vermieden werden, indem verschiedene, vielfältige (diversitäre) Berater, Hersteller, Analytiker, Monitoringsysteme parallel eingesetzt werden.

TAG 3 - Mit DevOps Netzwerkbereitstellung unterstützen

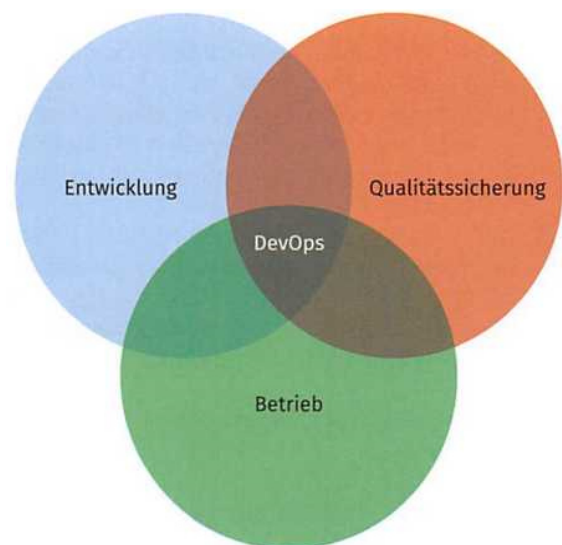
Bereitstellungen von Netzen werden in diesem Lernfeld als einmalige, einzigartige Maßnahmen mit einem festen Terminplan betrachtet. Laufende Bereitstellungen, Provisierungen, Orchestration und Administration werden überwiegend und vertiefend in den Lernfeldern des Jahrgangsbandes 3 behandelt.

Im Zusammenhang mit Projektmanagement, Teamarbeit oder bereichsübergreifender Entwicklung wird vielfach der Ausdruck „DevOps“ verwendet. In Stellenportalen werden Mitarbeiter für die Stellenbezeichnung DevOp gesucht. Die meisten DevOps werden in Bereichen der Anwendungsentwicklung gesucht, eine größere Zahl auch in der Systemadministration, insbesondere mit Bezug auf Cloud-Technologien und virtuellen Systemen.

Die Notwendigkeit eines DevOps-Ansatzes bzw. einer DevOps-Kultur wurde zunächst in Software-Entwicklungsbereichen gesehen und erfolgreich umgesetzt. Aufgrund der Virtualisierung von Systemen und der hohen Entwicklungsgeschwindigkeit bei Cloud-Systemen, digitalen Plattform- oder Ökosystemen sowie offenen und voll integrierten Softwaresystemen wurden mittlerweile viele Ausgestaltungen und Rollen dieses Konzepts etabliert. Dank dem Open-Cloud-System „Kubernetes“, Docker-Services und DevOps-Methoden sind Unternehmen in der Lage, weit flexibler zu agieren, sodass Entwicklungsteams die Bereitstellung von Cloud-Infrastrukturen automatisieren, frühzeitig sicherer entwickeln und neue Softwareversionen schnell veröffentlichen können. Security-Experten in DevOps-Teams können dies bei einem Shift-Left-Ansatz unterstützen. Sicherheits- und Compliance-Tools werden eingesetzt, um eine risikoprüfte und sichere Bereitstellung zu ermöglichen. Da beim DevOps-Ansatz laufend neue Funktionen oder Updates integriert werden, ergeben sich auch laufend Mehrwerte in Funktion und Sicherheit.

Bei einem „Shift-Left“ wird eine Aktion, hier die IT-Sicherheitstests, schon in einem frühen Stadium des Entwicklungsprozesses eingebunden, um Fehler im Produkt zu finden, zu beheben und zu verhindern, anstatt mit der Prüfung von Sicherheitsanforderungen erst bis zum Schluss oder bis zur Nutzung und Sicherheitsvorfällen zu warten. Die Entwicklungsreihenfolge könnte z. B. „Anforderungen - Sicherheitstests - Design - Sicherheitstests - Coding/Orchestrierung - Sicherheitstests - Bereitstellung“ sein. Diese frühzeitige Berücksichtigung hat die Vorteile, dass Fehler und Folgefehler früher erkannt werden, die Entwicklungsgeschwindigkeit sich insgesamt beschleunigt, Sicherheitslücken schneller und rechtzeitig geschlossen werden können.

DevOps-Engineers oder -Mitarbeiter werden gesucht und eingesetzt, um in Teams zwischen Entwicklung (Development), Qualitätssicherung und Betrieb (Operations) zu vermitteln, in der schnellen Weiterentwicklung eine kontinuierlich hohe Qualität an die Entwicklungsprodukte und -Systeme sicherzustellen. Unternehmen stellen IT-Systemadministratoren mit DevOps-Erfahrung ein, um ihre IT-Infrastruktur, Systeme und Dienste kontinuierlich weiterzuentwickeln bzw. auf dem aktuell neuesten und sichersten Stand zu halten. Dazu ist es notwendig, Mitarbeiter zu beschäftigen, die sich sowohl auf der Entwicklungsseite als auch auf der Operations- oder Einsatzseite mit Administrations-, Orchestrierungs- und Monitoring Systemen auskennen.



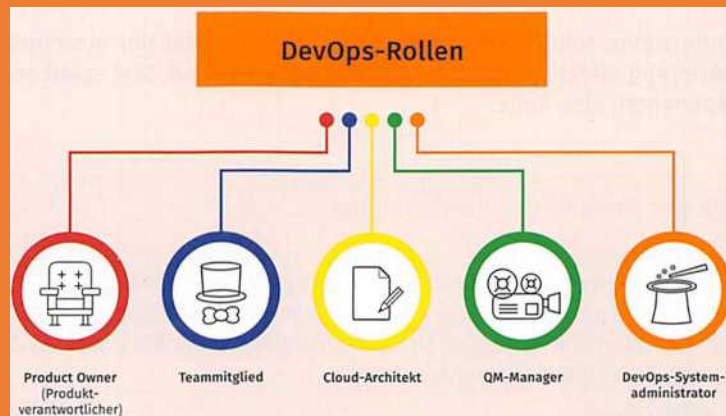
DevOps-Ansatz und –Kultur

Begriff

Der Begriff setzt sich aus „Development“ (Entwicklung) und „Operations“ (Vor-Ort-Einsatz) zusammen und bezeichnet eine Arbeitskultur zur Prozessverbesserung in der Softwareentwicklung und Systemadministration. Er wird als agiler Teamansatz eingesetzt, um die Bedeutung einer Zusammenarbeit von Entwicklung und Betrieb herauszustellen, dabei möglichst effizient, automatisiert und mit KI vorzugehen. DevOps-Praktiken wie Continuous Integration und Continuous Delivery sollen unter diesen Bedingungen zuverlässige Bereitstellungen ermöglichen. In Anpassung an unterschiedliche Entwicklungsbereiche werden unterschiedliche Ausgestaltungen vorgenommen, z. B. DevOps Engineer, Cross-Platform DevOps, Site Reliability Engineering (SRE), BizDevOps.

DevOps nach dem CALMS-Modell

C – Kultur(Culture)
A – Automatisierung
(Automation)
L – Schlank (Lean)
M – Messung (Measurement)
S – Austausch (Sharing)



DevOps-Prinzipien

- kundenorientiertes Handeln: Kundenerfahrungen besser berücksichtigen
- zielorientiertes Handeln: gemeinsam agil verantwortlich
- End-to-End-Verantwortung: im gesamten Produktlebenszyklus auch proaktiv
- funktionsübergreifende flexible Teams und plattformübergreifende (cross-plattform) Infrastrukturlösungen
- ständige Verbesserung: kontinuierliche Technologieanpassung und -Steuerung, in der Netzwerkbereitstellung durch Updates, Upgrades, Tests, Monitoring, Case-Management
- umfassende Standardisierung und Automatisierung, durch Monitoring, Automatisierung und Orchestrierung

DevOps Praktiken

- Kontinuierliche Integration (Continuous Integration): Sie beschreibt einen kontinuierlichen Prozess der Softwareentwicklung im Lebenszyklus. Die aktuellen Softwarequellen aller Entwickler werden automatisiert übersetzt und mit Unit-Tests getestet.
- Kontinuierliche Bereitstellung (Continuous Delivery): Sie enthält alle Schritte, um die Anwendungssoftware den Kunden bereitzustellen, also Packaging, Releasing, Configuring, Monitoring.

Die Bereitstellung von Netzwerken ist auch nach der Festlegung der Anforderungen und Vertragsunterzeichnung zwischen Auftraggeber und Auftragnehmer ein komplexer Vorgang. Zunächst muss die Netzwerkinfrastruktur eingerichtet oder auf den aktuellen Stand gebracht werden. Wenn die Materialien, Komponenten und Systeme beschafft sind, müssen eventuell Testinstallationen durchgeführt, die vereinbarte Form der Bereitstellung und Migration geplant sowie der Mitarbeitereinsatz organisiert werden.

Nach der Installation, Konfiguration und Provisionierung der Komponenten oder Orchestrierung der Systeme werden Maßnahmen festgelegt, um Vorgänge zur Administration zu automatisieren.

Um die Auswahl von IT-Komponenten und Orchestrierungen möglichst optimal und kostengünstig durchzuführen, werden Architekturmodelle zur Strukturierung und Nutzung verteilter Funktionalitäten wie SOI (Service Oriented Infrastructure) und SOA (Service Oriented Architecture der Anwendung) eingesetzt. SOI dient dabei der Orchestrierung von



Varianten der Netzwerkbereitstellung

virtualisierten Ressourcen (Rechner, Speicher, Netzwerke), SOA der Orchestrierung von Software und Daten in den Geschäftsprozessen.

SOA fordert eine sehr starke Integration und Flexibilität der einzelnen IT-Komponenten, damit deren Orchestrierung effektiv und kostengünstig gelingen kann. SOA spielt somit bereits bei der Auswahl von IT-Komponenten eine Rolle.

Varianten der Netzwerkbereitstellung

Architektur-Modelle im Cloud Computing (Webservices)

Enterprise Architecture (EA), Service Oriented Architecture (SOA), Service Oriented Enterprise Architecture (SOEA), Service Oriented Infrastructure (SOI), Service Oriented Enterprise (SOE), Service Oriented Management (SOM)

Konfiguration

- Damit ein Netzwerk funktioniert, müssen grundsätzlich drei Voraussetzungen erfüllt sein:
- Das richtige Protokoll (TCP/IP) muss auf den Geräten im Netz installiert sein.
- Jedes Gerät benötigt eine eigene IP-Adresse.
- Alle Geräte, die Daten austauschen, müssen derselben Arbeitsgruppe/dem IP-Adressbereich angehören.

Provisionierung (Anschaltung, virtuelle Bereitstellung)

Die zur Verwaltung des Zugriffs auf Daten und Ressourcen erforderlichen Schritte sowie deren Bereitstellung für Nutzer (Benutzerkonten) und Systeme werden i.d.R. als Provisionierung bezeichnet. Hersteller bieten für ihre Produkte (z. B. Microsoft Windows, Azure) Bereitstellungspakete an, die über Konfigurationsdiensteanbieter verfügbar sind. Über Tools (z. B. Asana) können Provisionierungen und Deprovisionierungen gemanagt werden.

Mit SCIM (System for Cross-domain Identity Management) ist ein offener Standard zur automatisierten Bereitstellung von Benutzerkonten zwischen Diensteanbietern verfügbar.

Der Begriff „Provisionierung“ wird für verschiedene Arten der Bereitstellung verwendet, z.B.

- **Serverprovisionierung:** umfasst das Einrichten der physischen Hardware in einem Rechenzentrum, das Installieren und Konfigurieren von Software, einschließlich des Betriebssystems und der Anwendungen, sowie das Verbinden mit Middleware, Netzwerken und Storage
- **Netzwerkprovisionierung:** umfasst das Einrichten eines Netzwerks (auch WLAN-Umgebung), auf das Nutzer, Server, Container und IoT-Geräte zugreifen können
- **Nutzerprovisionierung:** umfasst das Identitätsmanagement und die Überwachung der Zugriffs- und Autorisierungsrechte, z. B. für E-Mail, Datenbank- oder Netzwerkzugriffe
- **Serviceprovisionierung:** umfasst die Einrichtung eines Service und die Verwaltung der damit verbundenen Daten

Orchestrierung

Unter Orchestrierung versteht man die Komposition bzw. automatisierte Konfiguration, Verwaltung und Koordinierung von Computersystemen, virtuellen Systemen, Storage, Diensten, Prozessen, Services, Anwendungen, Webservices und Workflows. Damit können IT-Abteilungen komplexe Aufgaben effizienter bewältigen. Über die Orchestrierung werden den Prozessen und Diensten konkrete Aufgaben zugewiesen und die Abhängigkeiten untereinander gesteuert. Mit der Cloud-Orchestrierung werden Services unterschiedlicher oder gleicher Cloud-Umgebungen und -Anbieter zu einer Gesamtkomposition eingerichtet. Dafür werden i.d.R. Tools (z.B. „Docker“, „Kubernetes“, „ServiceNow“, „MS Configuration Manager“, „Red Hat Ansible“).

Automatisierung

Mit Automatisierung werden allgemein und mit der Netzwerkautomatisierung speziell Technologien und Verfahren eingesetzt, um weniger manuelle Aufgaben durchführen zu müssen. Dies betrifft die Administration bei Routern, Switches, Load Balancern und Firewalls sowie die aufwendigere manuelle Änderung der Konfiguration. Die Netzwerkautomatisierung erfolgt über Skripte, die auf der Befehlszeilenebene im Betriebssystem programmiert werden oder mittels Automatisierungssoftware. Beispiele in der Systembereitstellung sind: Infrastrukturautomatisierung, Cloudautomatisierung, Netzwerkautomatisierung, IT-Sicherheitsautomatisierung, Patch-Management-Automatisierung etc.

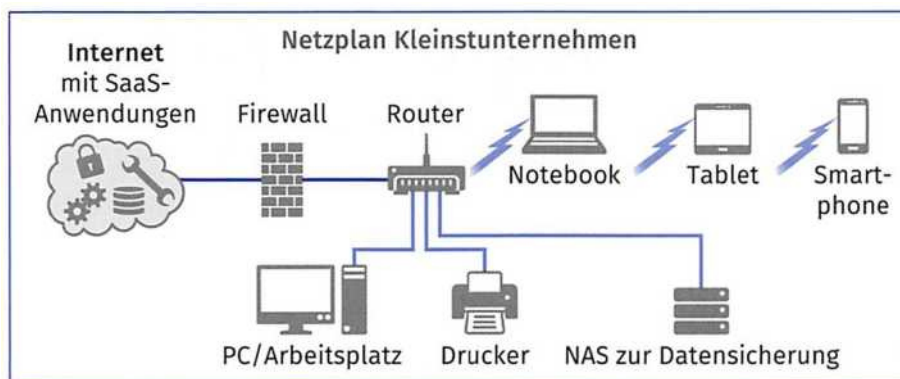
LE 1 - Ist-Analyse durchführen und Lastenhefte erstellen

Die Netzwerkbereitstellungen sollen aus der Sicht einer IT-Abteilung (interner Kunde) oder eines Systemhauses beschrieben werden, die Kundenaufträge von externen Kunden ausführen. Liegen Kundenaufträge von internen oder externen Kunden vor, ist der Kunde nach einem Lastenheft, nach einer Anforderungsliste etc. zu befragen und i.d.R. auch eine Ist-Analyse durchzuführen.

In den nächsten Lerneinheiten werden drei Kundengruppen unterschieden: Kleinstunternehmen, kleine mittelständische Unternehmen (KMU) und Großunternehmen. Kleinstunternehmen haben üblicherweise ein Büro, KMU ein oder mehrere Gebäude an einem Standort und Großunternehmen viele Standorte mit vielen Gebäuden. Diese Unterscheidung soll als Hilfe dienen und nicht als strikte Rahmenbedingung: In der Praxis zeigt sich, dass die Grenzen verschwimmen. So gibt es auch Kleinstunternehmen mit mehreren Büros und KMU, die an mehreren Standorten vertreten sind. Zu jeder Kundengruppe findet sich ein Beispiel für ein Lastenheft.

LE 2 - Kleine Netzwerke für Kleinstunternehmen planen

Bei der Kundengruppe der Kleinstunternehmen handelt es um Freiberufler und Solo-Selbstständige, rechtlich häufig um Einzelunternehmen.



Kleinstunternehmen haben für ihre Anwendungsfälle Programme zur Fakturierung (Auftragsbearbeitung, Rechnungserstellung), eine fachliche Software (z. B. ein Architekturprogramm) und Kommunikationssoftware/Groupware im Einsatz.

Typische Merkmale eines Kleinunternehmens sind häufig ein Büro, ein SoHo-Router, z. B. ein Speedport der Telekom oder AVMs Fritz!Box, mehrere Endgeräte wie PC, Laptop, Tablet, Smartphone und Drucker, welche über LAN oder WLAN mit dem Router verbunden sind, ein NAS für die lokale Datensicherung und mehrere SaaS Lösungen.

Viele SoHo-Router nutzen dynamische IP-Adressen. Der SoHo-Router erhält dabei alle 24 Stunden eine neue IP-Adresse.

Lastenheft Kleinunternehmen - *Beispiel*

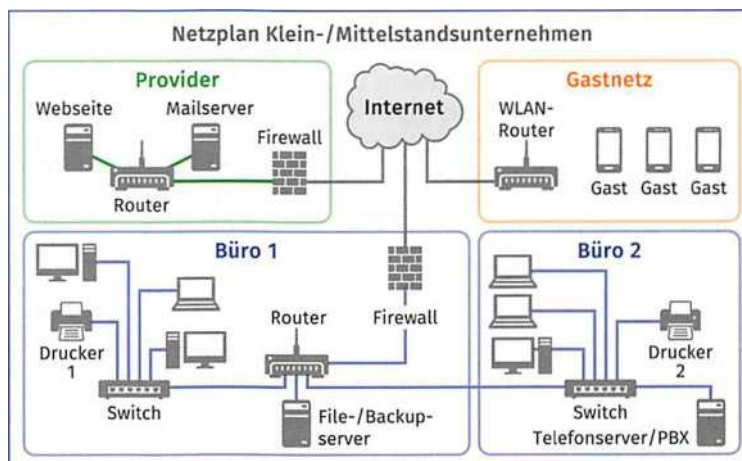
In der folgenden Vorlage hat der Auszubildende der JIKU IT-Solutions die Anforderungen des Kunden nach dem telefonischen Erstkontakt und einem Kundengespräch vor Ort erfasst. Sie dient der späteren Planung und dem Erstellen des Pflichtenheftes.

Lastenheft – Kleinunternehmen – 	
Kriterien	Anforderungen des Kunden
Ausgangssituation analysieren und Zielsetzung	<i>Firma Müller aus Hagen benötigt einen LTE WAN Router inkl. Einrichtung in den Büroräumen; DSL, WLAN und Netzwerkverkabelung (Switch) sind vorhanden; Kunde nutzt Webseite, Shop, E-Mail und Videokonferenzen; DSL soll wegen schlechter Qualität abgelöst werden; Telefonie läuft über Mobilfunk</i>
Funktionale Anforderungen (Muss- und Kann-Kriterien)	<i>Es werden mind. 10 MBit/s im Download, mind. 5 Mbit/s im Upload gewünscht; ein Anbieter (Provider) ist für Büroort zu ermitteln; Router muss DHCP- und DNS-Server mitbringen</i>
Nicht funktionale Anforderungen (Qualität, Administration, Compliance)	<i>Anlage vor Ort einrichten und die Konfiguration dokumentieren</i>
Sicherheit und Datenschutz	<i>LTE-Router soll über eine Firewall verfügen: ausgehende Verbindungen erlauben, eingehende verhindern</i>
Lebenszyklus des Netzwerksystems (Wartung, SLA)	<i>Vorhandener Router soll abgelöst werden; Provider-Vertrag bereits gekündigt; Support ist erwünscht, gerne per Video-call</i>
Lieferumfang (Zeit, Umfang, Dokumentation, Abnahmekriterien)	<i>Angebot erwünscht mit Einrichtungspreis, monatliche Kosten LTE und Support Pakete JIKU IT-Solutions, Auszubildender, 10.09.20..</i>

LE 3 - Mittlere Netzwerke für KMU und mittelgroße Organisationen planen

Die Kundengruppe der KMU umfasst Kunden mit bis zu ca. 100 Mitarbeitern. Es sind Rechtsformen wie z. B. die GmbH. Diese Kundengruppe hat oft nur einen Standort mit einem oder mehreren Gebäuden. Lokale Server sind vorhanden, die IT wird häufig von der Geschäftsführung gemangelt. Ab ca. 60 Mitarbeitern gibt es eigene Administratoren und i.d.R. einen Serverraum.

Im nebenstehenden Schaubild betreibt der Kunde ein Gastnetz für seine Kunden. Dieses Gastnetz stellt er über einen LTE-/WLAN Router seinen Kunden zur Verfügung.



Lastenheft KMU – Beispiel

In der folgenden Vorlage hat die Auszubildende der JIKU IT-Solutions die Anforderungen eines typischen KMU-Kunden nach einem Kundengespräch vor Ort erfasst.

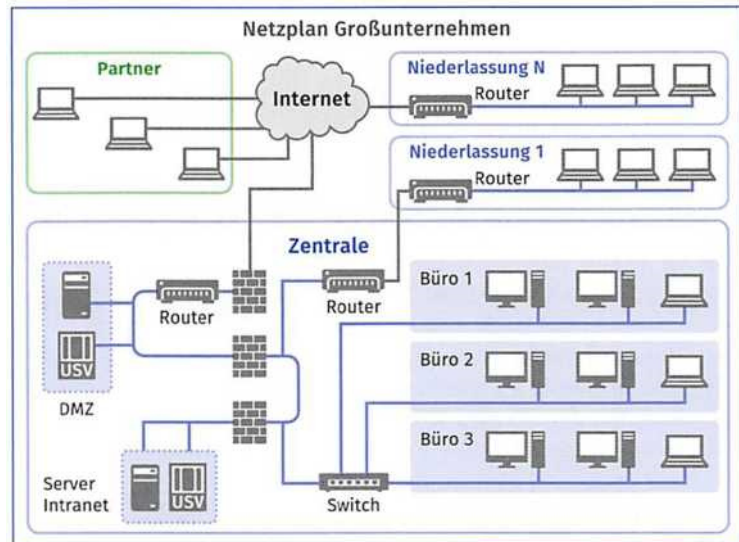
Lastenheft – Kleine u. mittlere Unternehmen (KMU) –	
Kriterien	Anforderungen des Kunden
Ausgangssituation analysieren und Zielsetzung	Die Maier GmbH aus Bayreuth benötigt ein CRM inkl. Telefonintegration und Einrichtung: bei eingehenden Anrufen soll der Anrufername auf den Mitarbeiterbildschirmen angezeigt werden. Es gibt 10 interne Mitarbeiter, 5 Bildschirme (Mitarbeiter arbeiten in zwei Schichten) und 50 mobile Mitarbeiter.
Funktionale Anforderungen (Muss- und Kann-Kriterien)	Wichtig ist die Telefonintegration: Bei eingehenden Anrufen soll jeder Büromitarbeiter den Kundennamen sehen, sodass der zuständige Mitarbeiter den Anruf entgegennimmt und im CRM sehen kann, was zuletzt mit dem Anrufer besprochen wurde. Die Inhalte des Gesprächs speichert der Mitarbeiter als Notiz im CRM.
Nicht funktionale Anforderungen (Qualität, Administration, Compliance)	Alle 5 Mitarbeiterplätze inkl. IP-Telefone und Telefonanlage müssen eingerichtet werden, möglichst an einem Wochenende ab Freitagnachmittag. Die Sicherung der VM soll auf bereits vorhandenem RAID-Server erfolgen.
Sicherheit und Datenschutz	Aus Datenschutzgründen soll ein lokaler Server mit CRM-VM aufgesetzt werden.
Lebenszyklus des Netzwerksystems (Wartung, SLA)	Support wird bei Bedarf remote gewünscht.

Kriterien	Anforderungen des Kunden
Lieferumfang (Zeit, Umfang, Dokumentation, Abnahmekriterien)	Angebot für CRM-Server inkl. Einrichtung und Wartung JIKU IT-Solutions, Auszubildende, 20.09.20..

LE 4 - Große Netzwerke für Mittel- und Großunternehmen planen

Große Unternehmen besitzen meist mehrere Niederlassungen. Rechtlich handelt es sich dabei oft um Aktiengesellschaften. Die verschiedenen Standorte sind über Router miteinander verbunden. Die Sicherheit wird über mehrere Firewalls erreicht:

- Anwendungen, die auch von Vertriebspartnern, Kunden und Lieferanten genutzt werden, befinden sich in einer sogenannten DMZ (Demilitarized Zone).
- Unternehmenskritische Anwendungen werden über eine weitere Firewall gegenüber dem Intranet geschützt. Die eingesetzten Firewalls kommen von unterschiedlichen Herstellern.
- Mehrere Administratoren sorgen für den reibungslosen Betrieb.
- Die Server der Großunternehmen sind über statische IP-Adressen aufrufbar.



Lastenheft Großunternehmen - Beispiel

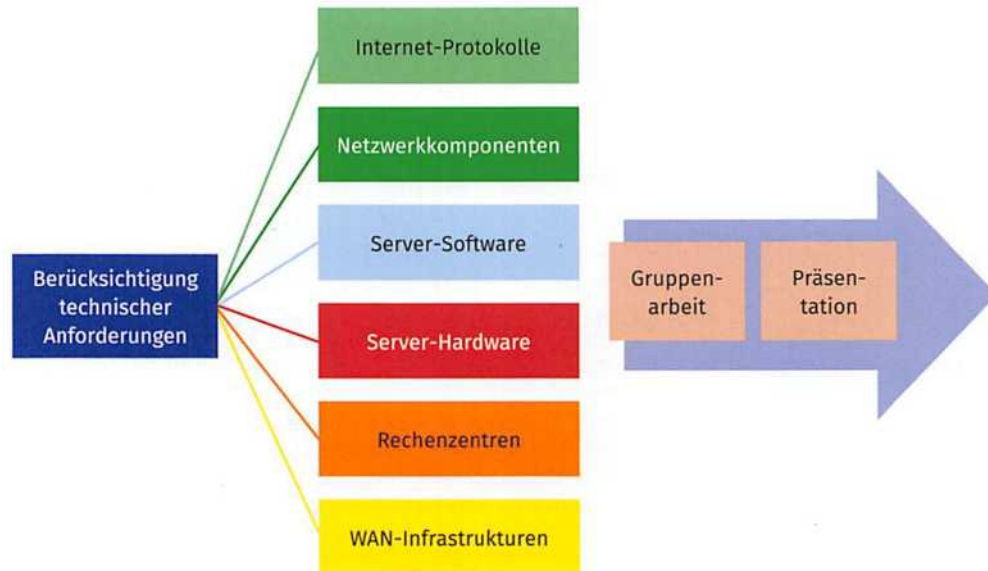
In der folgenden Vorlage hat der Auszubildende der JIKU IT-Solutions die Anforderungen eines Großkunden nach einem Kundengespräch vor Ort erfasst.

Lastenheft – Großunternehmen – JIKU IT-Solutions	
Kriterien	Anforderungen des Kunden
Ausgangssituation analysieren und Zielsetzung	Die Global AG aus Berlin möchte ihr verteiltes Rechenzentrum erweitern und einen zusätzlichen Hosters „ins Boot“ holen. Dieser soll seinen Sitz und sein Rechenzentrum in Deutschland haben. Bei diesem Hosters ist folgender Prototyp zu erstellen: ein virtueller dedicated Server, „Proxmox“ als Cloud-Software und zwei VM: einmal die Anwendung „Nextcloud“ und einmal eine Open-Source-Videookonferenzlösung, z. B. „jitsi“ oder „Work-Adventure“.
Funktionale Anforderungen (Muss- und Kann-Kriterien)	Beide Anwendungen sollten aus dem Internet heraus über https erreichbar sein. Die URLs werden noch bekannt gegeben. Innerhalb der „Nextcloud“ soll die App Deck zur Nutzung von Kanban-Boards eingerichtet werden.

Kriterien	Anforderungen des Kunden
Nicht funktionale Anforderungen (Qualität, Administration, Compliance)	<i>Der Kunde möchte die Admin-Rolle innerhalb der "Nextcloud"-Anwendung erhalten. Die technische Administration von „Proxmox“ und den VM verbleibt bei JIKU IT-Solutions.</i>
Sicherheit und Datenschutz	<i>Die VM sind mit Firewalls zu schützen. Noch Möglichkeit ist die Videokonferenzlösung mit einer Benutzerverwaltung zu versehen.</i>
Lebenszyklus des Netzwerksystems (Wartung, SLA)	<i>Updates in „Proxmox“ und den VM sind durch JIKU IT-Solutions durchzuführen.</i>
Lieferumfang (Zeit, Umfang, Dokumentation, Abnahmekriterien)	<i>Der Kunde erhält die URLs für die Anwendungen "Nextcloud" und „jitsi“ und Zugangsdaten für die „Nextcloud". JIKU IT-Solutions, Auszubildender, 05.10.20..</i>

TAG 4 - Technische Anforderungen für das Bereitstellen von Netzwerken berücksichtigen

Um Pflichtenhefte erstellen zu können, Ist-Analysen zu erstellen, Feinkonzepte zu entwerfen, sind aktuelle und detaillierte technische Informationen und Kompetenzen notwendig. Ergänzend zu den erreichten Kompetenzen aus den sollen weitere Kompetenzen zu Protokollen, zu Server- Hardware und -Software, Rechenzentren sowie WAN-Infrastrukturen erarbeitet werden.



LE 1 - Internet-Protokolle unterscheiden

Der weltweite Standard für das „Internet“ sind die Kommunikationsprotokolle in der Version 4 (IPv4) und in der Version 6 (IPv6). Beide Protokolle laufen parallel und es wird sicherlich noch viele Jahre dauern, bis IPv6 das alte Protokoll IPv4 vollständig ersetzt.

Die folgende Tabelle zeigt die wesentlichen Unterschiede von IPv4 zu IPv6.

Vermittlung/Routing von Nachrichten (Layer 3)	
Eigenschaften von IPv4 und IPv6 im Vergleich	
IPv4	IPv6
32 Bit großer Adressraum	128 Bit großer Adressraum
2^{32} mögliche Adressen $\approx$ 4,3 Milliarden Adressen	2^{128} mögliche Adressen $\approx$ 340 Sextillionen Adressen
dezimale Darstellung	hexadezimale Darstellung, 8 Blöcke á 16 Bit
<i>Beispiel:</i> 192.168.178.69	<i>Beispiel:</i> fe80::e022:d9bc:318b:1d7a <i>Hinweis:</i> Mit Nullen zwischen den Doppelpunkten :: auffüllen, sodass es 8 Blöcke á 16 Bit sind, also: fe80:0000:0000:0000:e022:d9bc:318b:1d7a
IPsec ist optional	IPsec ist optional
Checksummen erforderlich	keine Checksummen

Eigenschaften von IPv4 und IPv6 im Vergleich	
IPv4	IPv6
NAT erforderlich (Network Address Translation), um zusätzliche Adressen nutzen zu können	IPv6 kommt ohne NAT aus!
Paketgröße 576 Bytes	1280 Bytes
Fragmentierung von Nachrichten möglich, wenn ein Netzwerksegment eines Routers eine kleinere Paketgröße hat	keine Fragmentierung von Nachrichten; Router werden mit IPv6 entlastet

Das Internet-Protokoll stellt eine Vereinfachung des ISO/OSI-Referenzmodells dar.

Adressierung im Internet Protokoll		
OSI Schicht	TCP/IP	Beispiele
7 Anwendung	Anwendung	dhcp, dns, ftp, ftps, http, https, imap, ntp, pop3, rtp, sip, scp, sftp, smtp, snmp, socks, ssh, xmpp
6 Darstellung		
5 Sitzung		
4 Transport	Transport	TCP, UDP, TLS, DTLS
3 Vermittlung	Internet	IP: IPv4/IPv6, IPsec, ICMP, BGP, RIP
2 Sicherung	Netzzugang	ARP/NDP, PPP, PPPoE, MAC Adresse Ethernet, Token Ring, Glasfaser, WLAN
1 Bitübertragung		

Die Netzzugangsschicht ist eine Zusammenfassung der OSI-Schichten „Bit-Übertragung“ und „Sicherung“ die Anwendungsschicht eine Zusammenfassung der OSI-Schichten „Sitzung“, „Darstellung“ und „Anwendung“.

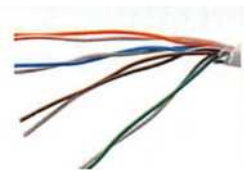
(1) Bitübertragung (OSI Layer 1)

Als Übertragungsmedien in den Unternehmensnetzen kommen am häufigsten das Ethernet-Kabel, WLAN und Glasfaserkabel vor.

Ethernet-Kabel

Bei der Verkabelung kommen Ethernet-Kabel am häufigsten zum Einsatz. Abschirmungen dienen dazu, ein „Übersprechen“ zu verhindern. Ethernet-Kabel bestehen aus sogenannten symmetrischen Leitungen. Dabei sind jeweils zwei Drähte zu einem Paar verdreht. Ein Netzkabel besteht aus vier verdrehten Aderpaaren. Je nach Art der Abschirmung werden folgende Ethernet-Kabel unterschieden:

Ethernet-Kabel - Art der Abschirmung	
UTP (Unshielded Twisted Pair)	Dieses ungeschirmte Kabel kommen als Fast- und Gigabit-Ethernet zum Einsatz. Die Kabel werden auch CAT5e-Kabel genannt.
STP (Shielded Twisted Pair)	Diese Bezeichnung besagt, dass eine Abschirmung vorhanden ist, aber nicht welche (adern paarweise oder gemeinsame Abschirmung).



Ethernet-Kabel - Art der Abschirmung	
S/STP (Screened Shielded Twisted Pair)	Dieses Kabel ist einzeln und über ein gemeinsames Geflecht abgeschirmt. 
S/FTP (Screened/Foiled shielded Twisted Pair)	Eine Folie wird für den Gesamtschirm genutzt. S/FTP kommt bei CAT7-Kabeln zum Einsatz, also bei 10 GBASE-T-Verkabelungen und ebenso bei CAT6a-Kabeln.

Als Stecker und Buchsen werden RJ45 benutzt. Die Gebäudeverkabelung läuft in einem Raum zusammen. Hier werden sogenannte Patch Panels eingesetzt. Auf der Rückseite werden die Netzwirkabel des Gebäudes einzeln „verdrahtet“. Auf der Vorderseite (siehe Abbildung unten rechts) lassen sich die Ports nun mit beliebigen Switches zu VLANs oder einem LAN verbinden.



RJ45-Stecker



RJ45-Anschlussdose



Patch Panels, Vorderseite

WLAN

Beim WLAN wird ein Funknetz aufgebaut und darüber werden Nachrichten gesendet und empfangen. Das Verfahren, wer wann senden darf, regelt die Sicherungsschicht. Die Internet Engineering Task Force hat mehrere Spezifikationen für das WLAN erstellt. Die maximale Datenübertragungsrate wurde bei jedem neuen Standard erhöht.

WLAN ist nicht gleich WLAN! Jeder neue Standard ist abwärtskompatibel. Der parallele Betrieb, z. B. von Geräten nach 802.11 g und 802.11 ac, ist erlaubt.

WLAN-Standards und ihre maximalen Datenübertragungsraten	
IEEE 802.11a	max. Datenraten von bis zu 54 MBit/s im 5 GHz Band
IEEE 802.11b	max. Datenraten von bis zu 11 MBit/s im 2,4 GHz Band
IEEE 802.11g	max. Datenraten von bis zu 54 MBit/s im 2,4 GHz Band
IEEE 802.11n	Wi-Fi4 erlaubt bis zu 289 MBit/s im 2,4 GHz Band und bis zu 600 MBit/s im 5 GHz Band
IEEE 802.11ac	Wi-Fi5 erreicht einen theoretischen Datendurchsatz von bis zu 6933 Mbit/s
IEEE 802.11ax	Wi-Fi6 ist der kommende Standard; liefert einen theoretischen Datendurchsatz von bis zu 9600 Mbit/s

Verkabelung mittels Lichtwellenleiter

Die Verkabelung mittels Lichtwellenleiter wird überall dort vorgenommen, wo höchste Datenübertragungsraten erreicht werden sollen (10 Gbit/s und größer), z.B. in Rechenzentren. Lichtwellenleiter-Patchkabel gibt es für verschiedene Fasertypen.



Verkabelung mittels Lichtwellenleiter



Patchkabel

Fibre-Channel-Verkabelung

Fibre Channel wurde speziell für Storage Area Networks (SAN) entwickelt. Zum Einsatz kommen hier Glasfaserkabel, über die dann der Fibre Channel Protocol Stack läuft.

(2) Sicherungsschicht (OSI Layer 2)

Die Sicherungsschicht ist dafür zuständig, die Übertragung der Nachrichten zu sichern. So legt das Verfahren CSMA/CD (Carrier Sense Multiple Access/Collision Detection) fest, wie auf einem gemeinsam Übertragungsmedium jeder „senden“ darf: „Horche eine zufällige Zeitspanne auf der Leitung und starte mit dem Senden, wenn kein anderes Gerät gerade sendet. Direkt nach dem Senden horche, ob jemand parallel am Senden war, falls Ja, dann sende ein Jam-Signal“, siehe auch Lernfeld 3, Seite 300.

(3) Adressierung (OSI Layer 3)

Jeder Client im Internet, z. B. PC, Smartphones oder Tablets, besitzt eine IP-Adresse, um eine Anwendung auf einem Server (auch dieser hat eine IP-Adresse) „aufrufen“ zu können. Beispielsweise wird beim Aufruf einer Webseite mit einem Browser eine HTTP-Anfrage erstellt. Diese enthält die Sender-IP-Adresse des Clients, die Empfänger-IP-Adresse des Webservers und den Port, z. B. 443, bei einer dynamischen Webseite. Entscheidend für die Adressierung sind die MAC-Adresse der Netzwerkkarten, IPv4- und IPv6-Adressen der Clients und Server und die Port-Nummern der Dienste.

Adressbestandteile			
Adresse	Aufbau	OSI-Schicht	Nutzung
MAC	48 Bit, Hex-Schreibweise (byteweise), z.B.: EA-B1-FC-03-2D-0C	Layer 2 Datalink-Schicht	Über die MAC-Adresse werden die Netzwerkkarten im Netz eindeutig identifiziert.
IPv4	32 Bit, Dezimalschreibweise (byteweise) als 4 8-Bit-Zahlen, z.B.: 192.168.0.97	Layer 3 Netzwerk-Schicht	Jeder Rechner ist über die IP-Adresse identifizierbar. IPv4 und IPv6 sind parallel im Internet verfügbar (Dual Stack).
IPv6	128 Bit, Hexadezimalschreibweise (wortweise) als acht 16-Bit-Zahlen, z.B.: 2a02:8070:88a3:9d00:b519:89cb:afe1:1561	Layer 3 Netzwerk-Schicht	Jeder Rechner ist über die IP-Adresse identifizierbar. Die Umstellung auf IPv6 ist im Gange.
Port-Nummer	16 Bit, Dezimalschreibweise, z.B.: 43201	Layer 4 Transport-Schicht	Über den Port werden Anwendungen und Dienste adressiert.

MAC-Adressen

Bei den MAC-Adressen handelt es sich um die Hardware-Adresse der Netzwerkkarte bzw. physikalische Adresse.

MAC-Adressen (Media Access Control) bestehen aus der Hersteller-Kennung (Vendor-ID) und einer fortlaufenden Nummer.

IPv4-Adressen

IPv4-Adressen bestehen aus Netz-Adresse und Host-Adresse. Große IP-Netze bestehen aus einem kleinen Netz- und einen großen Host-Anteil

Schreibweise:

Zwei Schreibweisen sind möglich, IP-Adresse mit Subnetzmaske in Dezimalschreibweise und in CIDR- oder Slash-Notation. Das folgende Schaubild zeigt, wie sich die IP Adresse 10.1.1.2 in Netz- und Hostadresse aufsplittet:

</>	0000 1010.0000 0001.0000 0001 . 0000 0010	IP-Adresse	10 . 1 . 1 . 2
	1111 1111.1111 1111.1111 1111 . 0000 0000	Subnetzmaske	255.255.255.0
	Netz-Adresse	Host-Adresse	

Die Netz-Adresse steht immer links, die Host-Adresse immer rechts. Bei der Dezimalschreibweise werden die IP-Adresse und die dazugehörige Subnetzmaske mit jeweils vier durch Punkte getrennte Dezimalzahlen dargestellt. Dabei steht eine 1 in der Subnetzmaske für ein Netz-Bit und eine 0 für ein Host-Bit.

Bei der CIDR-Notation wird die Anzahl der Bits, die die Netzwerkadresse darstellen, der IP angehängt. Die IP-Adresse 10.1.1.2 mit Subnetzmaske 255.255.255.0 verfügt über 24 Netz-Bits und wird in der neueren Schreibweise 10.1.1.2/24 geschrieben. Diese Schreibweise nennt man auch Slash-Notation. Die angehängte Zahl wird als Präfix bezeichnet.

Ein Class-A-Netzwerk besteht aus 8 Netz-Bits und 24 Host-Bits. Damit wären 16777 216 Adressen (2^{24}) möglich!

</> NNNN NNNN.HHHH HHHH.HHHH HHHH.HHHH HHHH

Ein Class-B-Netzwerk besteht aus 16 Netz-Bits und 16 Host-Bits. Damit sind 65 536 Adressen (2^{16}) möglich.

</> NNNN NNNN.NNNN NNNN.HHHH HHHH.HHHH HHHH

Zum Berechnen der Netzadresse werden aus der IP-Adresse diejenigen Bits verwendet, bei denen in der Subnetzmaske eine „1“ steht. Die Host-Bits werden auf null gesetzt. Die Anzahl der 1en in der Subnetzmaske wird in der CIDR-Schreibweise durch einen Schrägstrich getrennt an die IP-Adresse angehängt. Zum Berechnen der Hostadresse werden aus der IP-Adresse diejenigen Bits derjenigen Stellen verwendet, bei denen in der Subnetzmaske eine „0“ steht.

IPv6-Adressen

IPv6-Adressen bestehen aus 128 Bits, der Header hat eine Länge von 40 Bytes.

IPv4-Adresse				IPv6-Adresse													
Byte1	2	3	4	Wort 1	2	3	4	5	6	7	8	9	10	11	12	13	14
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx	xxxx
10 . 1 . 1 . 2				20 fe	af fe	00 00	00 00	01 23	45 67	89 ab	cd ef						
32 Bit				128 Bit													

IPv6-Adressen werden in das sogenannte Präfix und den Interface Identifier aufgeteilt. Beide haben eine Länge von 64 Bit.

Schreibweise:

1. Führende Nullen können weggelassen werden. So wird aus 20fe:affe:0000:0000:0123:4567:89ab:cdef schließlich:

```
</> 20fe:affe::123:4567:89ab:cdef
```

2. Ein (und nur ein) zusammenhängender Block Nullen kann durch Doppel-Doppelpunkt (::) ersetzt werden.

```
</> ::ffff:10.0.1.1 oder ::ffff:a011
```

Die Anzahl der Nullen beim :: wird so aufgefüllt, dass die Adresse 128 Bit hat. Damit ist die Anzahl der durch den Doppel-Doppelpunkt ersetzten Nullen nicht klar. Diese Regel darf deshalb nur einmal angewendet werden!

3. In die letzten zwei Blöcke kann auch die IPv4-Adresse eingesetzt werden. Diese kann wahlweise in Hex oder in Dezimal geschrieben werden. Dies wird angewendet, wenn ein IPv4-Adressraum in einen IPv6- Adressraum eingebettet wird. Die IP 10.0.1.1 kann dann als IPv6-Adresse wie folgt geschrieben werden:

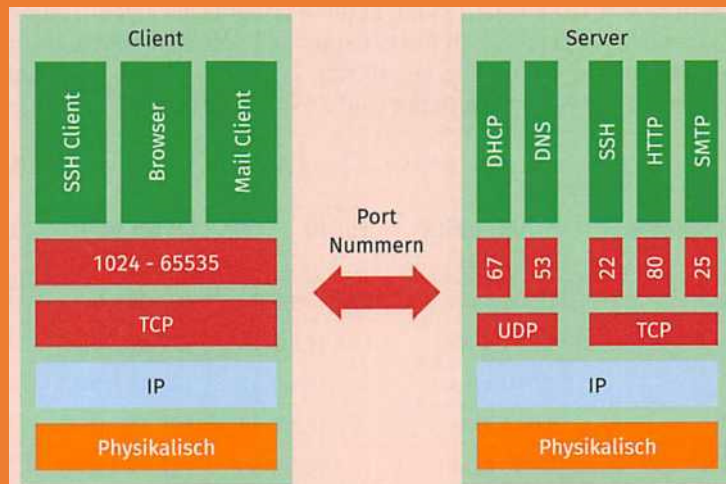
```
</> 20fe:affe:0:0:123:4567:89ab:cdef
```

Die Adresse 2001:0db8:1234:0000:0000:0000:0000/48 bezeichnet das Netz 2001:0db8:1234 mit dem Adressbereich 2001:0db8:1234:0000:0000:0000:0000 bis 2001:0db8:1234:ffff:ffff:ffff:ffff. Die ersten 48 Bit der Adresse entsprechen dem Netzanteil.

Port-Nummern

Port-Nummern dienen dem Adressieren von Diensten. Ein Port ist eine 16-Bit-Zahl. Sowohl der Absender als auch der Empfänger nutzen einen Port zur Festlegung der zuständigen Anwendung. Der Empfänger einer IP-Nachricht (Transportschicht, Layer 4) leitet die empfangende Nachricht an die registrierte Webanwendung (Anwendungsschicht, Layer 5 bis 7) weiter. Über den Mechanismus der „Ports“ können

auf dem Client gleichzeitig mehrere Anwendungen Nachrichten senden und auf den Servern gleichzeitig mehrere Server-Anwendungen Nachrichten empfangen. So können auf einem physikalischen Server parallel ein Webserver, ein Mail-Server, ein Videokonferenzsystem u.v.m. laufen. Auf dem Client können gleichzeitig ein Browser, ein E-Mail-Programm, ein Videokonferenz-Client etc. laufen.



Ports bekannter Webanwendungen (Auswahl)	
Port	Bedeutung
22	SSH, Secure Shell
53	DNS, das <i>Domain Name System</i> ist hierüber erreichbar.
67/UDP, 68/UDP	DHCP, das <i>Dynamic Host Configuration Protocol</i> läuft über diese Ports.
80/443	http/https für statische und dynamische Webseiten
161/UDP	SNMP zur Steuerung von Netzwerkkomponenten
143	IMAP, das <i>Internet Message Access Protocol</i> , zum Empfangen von E-Mails von einem Mailserver
401	UPS, Uninterruptable Power Supply
445/TCP	Microsofts Windows Freigaben CIFS/SMB (Samba) zum Mounten/Verbinden von Windows-Laufwerken im Netzwerk
546/UDP, 547/UDP	DHCP für IPv6: Es wird nur UDP genutzt, kein TCP.

LE 2 - IP Subnetting und virtuelle LANs (VLAN)

Durch IP-Subnetting werden Netze in Teilnetze gegliedert. Ursprünglich sollten somit die knappen IPv4- Adressräume effizienter genutzt werden. Dabei bietet Subnetting weitere Vorteile, z. B. das Erhöhen der Sicherheit: Durch das Bilden von virtuellen LANs, sogenannten VLANs, können beliebige Hosts eines LANs einer logischen zusammenhängenden Gruppe, dem VLAN, zugeordnet werden. Nach entsprechender Konfiguration der Switches können nur noch diejenigen Hosts miteinander kommunizieren, die sich im selben VLAN befinden.

Man kann VLANs in einem Netzwerk mit einem einzigen Adressbereich einsetzen oder aber den IP- Adressbereich aufteilen und für jedes VLAN ein eigenes IP-Subnetz verwenden. Dazu wird das Netz in mehrere kleine Subnetze aufgeteilt. Die Anzahl der benötigten Subnetz-Bits hängt von der benötigten Größe der VLANs ab.

Beispiel:

Das Netzwerk 192.168.0.0/24 hat einen Hostbereich von 8 Bit. Damit sind 256 Adressen darstellbar. Wenn ein VLAN maximal 10 Hosts beinhalten soll, dann muss ein Hostbereich von 4 Bit übrigbleiben. Mit diesen 4 Host-Bits lassen sich $2^4 - 2 = 14$ Hosts adressieren. Es stehen somit 4 Bit zum Subnetting zur Verfügung. Damit sind $2^4 = 16$ Subnetze adressierbar.

N N N N' N N N N. N N N N' N N N N. N N N N' N N N N. S S S S ' H H H H

Subnet Nr.	Subnet Bits 4.Oktett	Net-ID	Erster Host	Letzter Host	Broadcast Subnet
0	0000 xxxx	192.168.0.0	192.168.0.1	192.168.0.14	192.168.0.15
1	0001 xxxx	192.168.0.16	192.168.0.17	192.168.0.30	192.168.0.31
2	0010 xxxx	192.168.0.32	192.168.0.33	192.168.0.46	192.168.0.47
3	0011 xxxx	192.168.0.48	192.168.0.49	192.168.0.62	192.168.0.63
4	0100 xxxx	192.168.0.64	192.168.0.65	192.168.0.78	192.168.0.79
14	1110 xxxx	192.168.0.224	192.168.0.225	192.168.0.238	192.168.0.239
15	1111 xxxx	192.168.0.240	192.168.0.241	192.168.0.254	192.168.0.255

Vermittlung bzw. Routing von Nachrichten (OSI Layer 3)

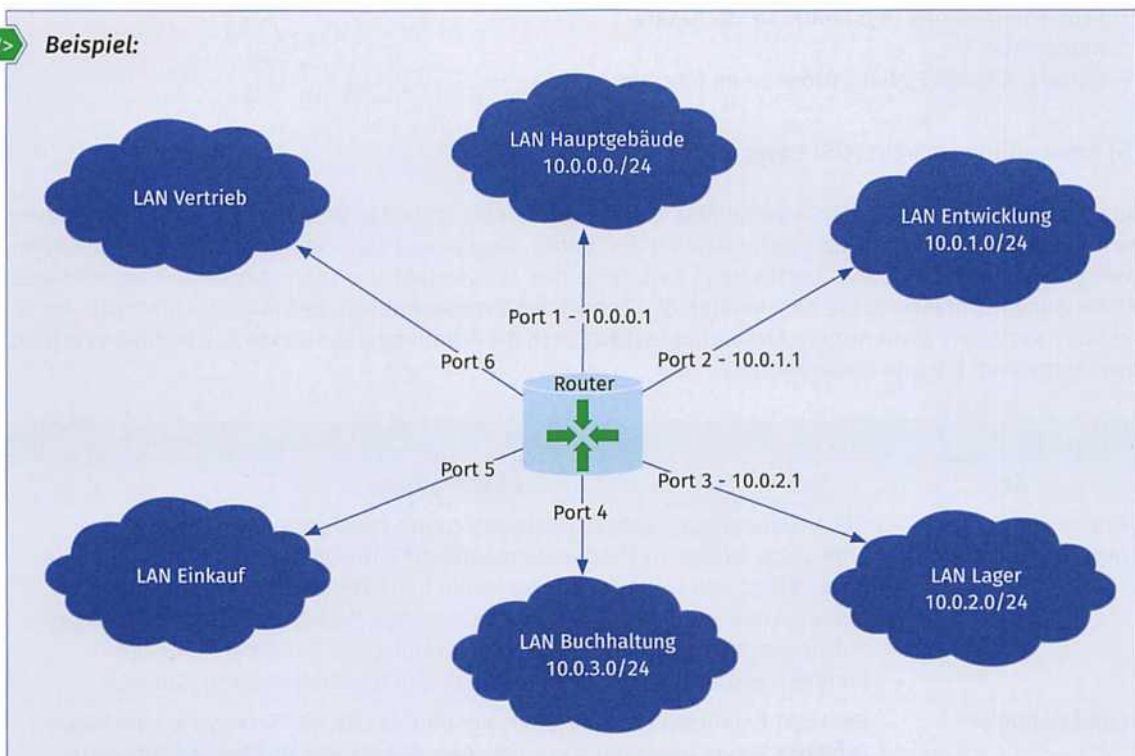
Routing

Routing beschreibt in der Netzwerktechnik das Verfahren zum Weiterleiten von Nachrichtepaketen. Befindet sich eine Zieladresse nicht im eigenen Netzwerk, so leitet der Router dieses Netzwerkes das Nachrichtenpaket an den nächsten Router weiter.

Router haben die Aufgabe, einen Weg durch das Netz gemäß der eigenen Routing-Tabelle zu wählen. Die Zieladresse jeder empfangenen Nachricht wird gegen die interne Weiterleitungs- und Routingtabelle geprüft. Die Nachricht wird entsprechend geroutet.



Beispiel:



In der Routing-Tabelle dieses Routers ist jedes Netz mit einem Eintrag vorhanden. Alle Netze sind direkt mit diesem Router verbunden. Die Routing-Tabelle für dieses Netz sieht vereinfacht wie folgt aus:

Netzwerk	Ausgabe-Port	IP-Adresse des Router-Ports	Bemerkungen
10.0.0.0/24	Port 1	10.0.0.1	Netz Hauptgebäude
10.0.1.0/24	Port 2	10.0.1.1	Netz Entwicklung
10.0.2.0/24	Port 3	10.0.2.1	Netz Lager
...	...		...

Für jedes ankommende IP-Paket sucht der Router anhand der Ziel-IP den passenden Router-Port aus der Tabelle aus und schickt das Paket an diesem Port weiter. Bei kleinen Netzwerken findet das Routing über statische Routing-Tabellen statt. Bei großen Netzwerken wird das Routing dynamisch durchgeführt: Jedes Nachrichtenpaket kann einen anderen Weg durch das Internet nehmen.

(4) Transport von Nachrichten (OSI Layer 4)

Die Aufgabe der Transportschicht-Protokolle UDP und TCP ist der Transport der Anwendungsdaten über die darunterliegende Vermittlungsschicht (IP, IPsec).

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
• Auf- und Abbau von Sitzungen • Zerlegen von Dateien oder Datenströmen der Anwendungen in einzelne Segmente • Zusammenfügen der Segmente in korrekter Reihenfolge und Wiederherstellung und Übergabe an die Anwendungen • Fehlerbehandlung und Kontrolle, ob Pakete ankommen • Einsatz, z.B. bei E-Mails, Browsen im Internet	• kein Auf- und Abbau von Sitzungen • Verschicken der Daten ohne jegliche Kontrolle und ohne Rückmeldung • Einsatz, z. B. bei Audio- und Video-streaming

(5) Anwendungsschicht (OSI Layer 5-7)

Aus der Zeit der Client-Server-Anwendungen, diese wurden bis Ende der 1990er-Jahre entwickelt, hatten sich Serverarten wie Back-up-, Datenbank-, File-/Datei-, Druck- und Mail-Server etabliert. Diese Server werden so nur noch selten „vertrieben“. Seit Ende der 1990er-Jahre werden stattdessen webbasierte Anwendungen entwickelt, die dem Kunden den Zugriff per Browser ermöglichen (auch Mehrschicht-Architekturen genannt). Nicht nur die Anwendung selbst, auch die Administration dieser Anwendungen erfolgt browserbasiert, z. B. per Smartphone.

Serverarten	
Art	Beschreibung
Anwendungsserver (Application Server)	Bei Anwendungsservern handelt es sich um Plattformen wie Oracles Java Enterprise Edition (JEE) oder Microsofts .NET. Diese erlauben eine schnellere Entwicklung von Webanwendungen durch die Trennung der Algorithmen in Modell, View und Control. Die Anwendung des Modell-View-Control-Design- Patterns ermöglicht die parallele Entwicklung von Datenbanktabellen (Modell), grafischen Oberflächen (View) und Geschäftslogiken (Control).
Load Balancer	Bei Load Balancern (Lastverteiler) handelt es sich um Server, die eine Skalierung der Serveranwendung ermöglichen. Sie dienen als Einstiegspunkt für Cluster. Ein Browser ruft eine URL auf, die von einem Load Balancer an einen Server im Cluster weitergeleitet wird. Alle Antworten und weiteren Anfragen dieses Browsers leitet der Load Balancer an diesen Server weiter.
Back-up-Server	Bei den Mehrschicht-Architekturen handelt es sich um Standby-Systeme, welche eingesetzt werden, sobald das Hauptsystem ausfällt.
Reverse Proxy	Ein Reverse-Proxy ist ein Stellvertreter für Anfragen aus dem Internet, welche dieser an mehrere interne Server verteilt. <i>Beispiel:</i> Die folgenden fiktiven Links www.meine-domain.de/anwendung1 und www.meine-domain.de/anwendung2 werden firmenintern von unterschiedlichen Servern bedient: auf www.meine-domain.de arbeitet ein Reverse-Proxy, der eingehende Nachrichten zu den Servern weiterleitet. Für den Anwender wirkt es, als würde lediglich ein Server die zwei URLs bedienen.

Kunden fokussieren sich auf Anwendungsfälle, die sie mit einer Software abdecken möchten und nicht mehr auf Installation, Konfiguration und Wartung.

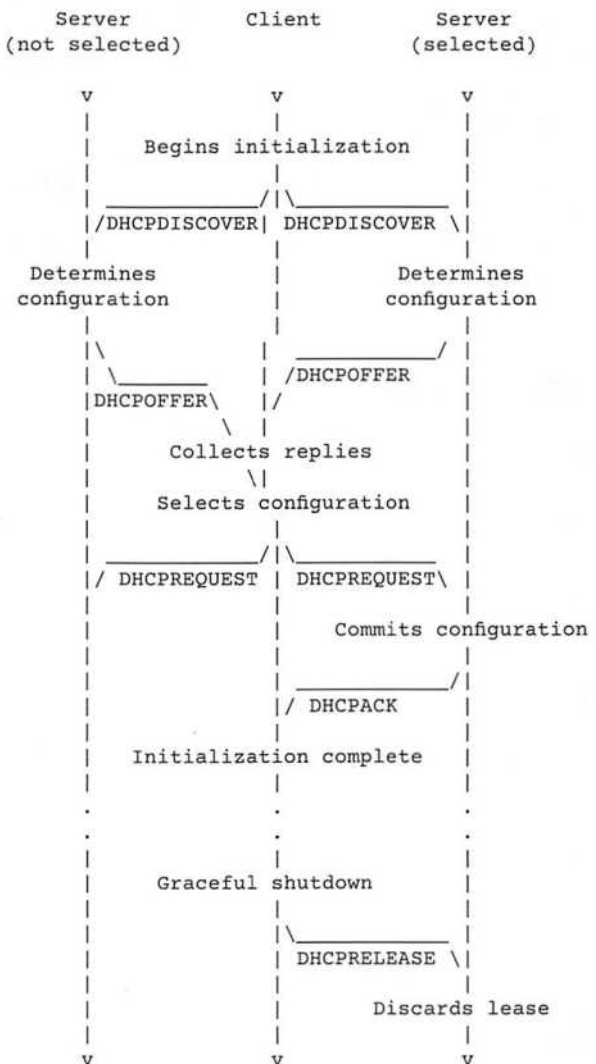
Beispiele für Anwendungsfälle	
Anwendungsfall	Beschreibung
CRM	Kundenmanagementsysteme, z.B. „SuiteCRM“ (https://suitecrm.com)
Zusammenarbeit	Systeme für die Zusammenarbeit, z.B. "CryptPad" (https://cryptpad.fr) und „Nextcloud“ (https://nextcloud.com)
Videokonferenz	z.B. „Jitsi“ (https://jitsi.org), „Nextcloud Talk“ (https://apps.nextcloud.com/apps/spreed) und „BigBlueButton™“ (https://bigbluebutton.org)
E-Mail-Marketing	E-Mail-Marketing erlaubt die gezielte Analyse von Kampagnen, z. B. „Mautic“ (https://www.mautic.org)
Mein Schulnetz	zeitgemäße Anwendungen für Schülerinnen und Schüler sowie Lehrkräfte auf einer "Proxmox"-Infrastruktur. Anwendungen sind „OPNsense“, „Nextcloud“ inklusive Chat, Telefonie, Videokonferenzen, Collabora-Online-Office, Kalender, Kontakte, getrennte VLANs für Schüler, Lehrer und Server u.v.m. (https://schulnetzkonzept.de)

DHCP-Dienst/-Server

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die automatische Einbindung von Geräten in ein bestehendes Netzwerk. Dabei bezieht der Client die IP-Adresse, die Netzmaske, den Name-Server und das Gateway automatisch.

Der Bezug dieser Information folgt dem Ablauf in der Abbildung. Der Client sendet ein sogenanntes DHCPDISCOVER als Broadcast in das lokale Subnetz und damit an alle darin befindlichen DHCP-Server. Die vorhandenen DHCP-Server senden nun ihre Angebote zurück als DHCPPOFFER Nachricht und inklusive einer Netzwerkadresse. Der Client entscheidet sich für ein Angebot und sendet ein DHCPREQUEST als Broadcast - darin befindet sich die Server-ID des gewählten DHCP-Servers. Der gewählte Server antwortet nun mit einem DHCPACK (acknowledge: bestätigen). Darin befinden sich die Konfigurationsparameter. Sollte der Client ein DHCPNAK empfangen, so startet er die Konfiguration erneut.

Ein entsprechender DHCP-Server bzw. -Dienst muss dafür aufgesetzt und konfiguriert werden. Ohne solch einen Dienst müssen die IP-Adressen an jedem Client manuell konfiguriert werden. Das DHCP ist in den RFC2131 der Internet Engineering Task Force (IETF) spezifiziert (siehe <https://tools.ietf.org/html/rfc2131>).



Zeitliche Abfolge der Nachrichten zwischen einem DHCP Client und Servern beim Aushandeln einer IP-Adresse

DNS - DynDNS

Das Domain Name System (DNS) zählt zu den wichtigsten Diensten des Internets. Es erlaubt den Anwendern, mit Rechnernamen und URLs zu arbeiten, welche von einem Nameserver (DNS- Dienst bzw. DNS-Server) aufgelöst werden. Das DNS ist in der RFC1034 und RFC1035 spezifiziert (siehe <https://tools.ietf.org/html/rfc1034>).

Möchte ein Anwender auf dem PC oder Smartphone beispielsweise eine Webseite anzeigen, z. B. www.westermann.de, so schickt das Betriebssystem eine DNS-Anfrage an den DNS-Server. Das ist oft der nächste Router. Dieser schickt die dazugehörige IP-Adresse zurück, in diesem Fall die 217.13.73.44. Der PC nimmt die IP-Adresse und erstellt damit sein http-Request.



DNS absichern

DNS läuft im Klartext (unverschlüsselt) und kann mitgelesen werden. Um DNS-Anfragen abzusichern, sollte DNS over TLS, DNS over HTTPS oder DNS over QUIC eingesetzt werden.

DynDNS

Viele Haushalte erhalten alle 24 Stunden eine neue IPv4-Adresse. Soll aus solch einem Haushalt ein interner Server im Internet verfügbar gemacht werden, so muss dieser Server seine neue IP-Adresse alle 24 Stunden bei einem DynDNS-Server aktualisieren. Dieser liefert bei Anfragen stets die aktuelle Adresse zurück.

Dynamic DNS Updates ist in der RFC2136 und RFC3007 spezifiziert (siehe <https://tools.ietf.org/html/rfc2136>).

TAG 5 - Netzwerkkomponenten unterscheiden

Alle eingesetzten Netzwerkkomponenten in einem Netzwerk müssen aufeinander abgestimmt sein. Dies gilt sowohl für aktive Netzwerkkomponenten, da sie über eine Stromversorgung verfügen, als auch für passive Netzwerkkomponenten. In diesem Kapitel werden die technischen Anforderungen an die Netzwerkkomponenten betrachtet.

LE 1 - Access Points

Access Points bzw. Wireless Access Points stellen Zugriffspunkte für Netzwerkgeräte dar. Über einen Access Point erhalten Smartphones, Laptops, Tablets etc. Zugriff auf ein Netzwerk. In Heimroutern ist ein Access Point oft integriert.

Folgende technische Anforderungen werden bei der Auswahl dedizierter Access Points berücksichtigt:

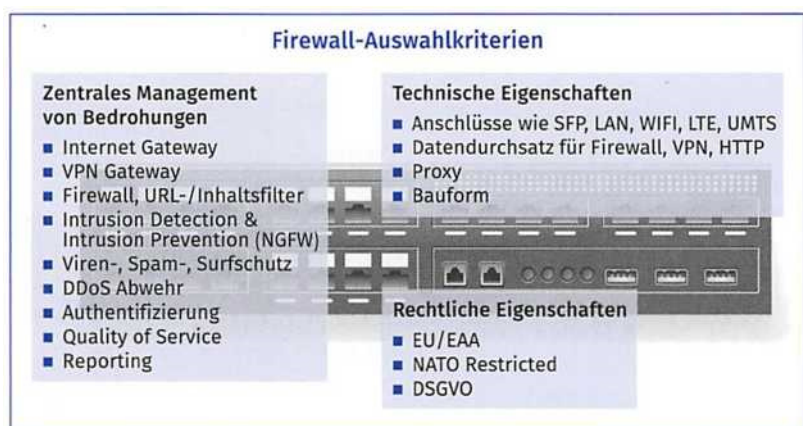


Technische Anforderungen an Access Points	
WiFi 6/WiFi 5	Die WiFi-Alliance spezifiziert die WLAN-Standards (siehe auch Tabelle „WLAN- Standards“).
WLAN-Geschwindigkeit	Neben dem theoretischen Datendurchsatz interessiert der tatsächlich verfügbare Datendurchsatz. Bei WiFi 5 sind dies 1 733 Mbit/s (Stand: 2021).
Dual WLAN	WLAN-Geräte nutzen entweder das 2,4-GHz und/oder das 5-GHz-WLAN.
MU-MIMO	Multiple Input - Multiple Output (MIMO) bezeichnet ein Verfahren zur Nutzung mehrerer Send- und Empfangsantennen. Es werden zusätzlich spezielle Codierungsverfahren eingesetzt mit dem Ziel, Qualität und Datendurchsatz der drahtlosen Verbindungen zu erhöhen. Mit Multi-User-MIMO (MU-MIMO) kann ein Access Point mehreren Clients gleichzeitig verschiedene Datensätze schicken.
OFDMA	Das Modulationsverfahren „Orthogonal Frequency-Division Multiple Access“ ermöglicht dem Sender, aufgrund bidirektionaler Kommunikation, die genutzten Kanäle zu messen. Damit kann der Access Point die Effizienz optimieren.
Multi-Gigabit-Ethernet	Es stehen mehrere Gigabit-Ethernet-Ports zur Verfügung.
Bridging- Funktion	Diese Access Points können als Bridge eingesetzt werden.
Stromversorgung über PoE	Diese Access Points werden über Power over Ethernet (PoE) mit Strom versorgt.
Leistung PoE/ PoE+-Ports	Da die Ports nicht überlastet werden dürfen, ist die maximale Leistung der PoE/ PoE+-Ports beim Anschluss von PoE-Geräten zu beachten. Diese sind für PoE und PoE+ unterschiedlich.

Technische Anforderungen an Access Points	
Ports 10/100/1000 BASE-T, RJ45	Ports mit höherem Datendurchsatz sind grundsätzlich zu bevorzugen. Die Angabe 10/100/1000 bezeichnet den Durchsatz in Mbit/s.
Einsatzbereich	Industrielle Access Points sind für größere Temperaturbereiche geeignet. Outdoor-Geräte sind vor Feuchtigkeit geschützt.
Abnehmbare Antennen	Abnehmbare Antennen bedeuten, dass diese durch andere Antennen getauscht werden können.
Gehäusebauform	Access Points werden in den unterschiedlichsten Gehäusebauformen angeboten.

LE 2 - Firewall

Eine Firewall ist eine Software, die in der Lage ist, eingehenden (schadhaften) Netzwerkverkehr zu filtern und zu blockieren, um damit ein ganzes Netzwerk zu schützen wie eine Brandmauer vor Feuer. Da Firewalls den Netzwerkverkehr niemals ausbremsen dürfen und Hardware grundsätzlich am performantesten läuft, werden Firewalls auch als dedizierte Hardware angeboten. In der Cloud werden Firewalls Virtualisiert betrieben.



Technische Anforderungen an Firewalls	
Internet Gateway	Firewalls werden so eingesetzt, dass sie den gesamten Datenverkehr, z. B. zwischen Intranet und Internet, als Gateway überwachen. Im einfachsten Fall steht ein Paketfilter zur Verfügung. Dieser filtert ganze UDP/TCP Nachrichten heraus aufgrund von Filterregeln für erlaubte/unerlaubte IP-Absenderadresse, IP-Zieladresse und Port. Firewalls mit „Stateful Paket Inspection“ speichern, welche offenen Verbindungen es gibt. So werden beispielsweise http-Antworten/Responses ohne dazugehöriger http-Anfrage/Request verworfen. Bei „Deep Paket Inspection“ werden die IP-Header analysiert und ggf. gefiltert.
VPN Gateway	Da Firewalls als Brandmauer für das interne Netzwerk eingesetzt werden, bringen sie oft eine VPN-Gateway-Funktion mit. Die maximale Anzahl gleichzeitiger VPN-Verbindungen ist in der Bewertung relevant.
URL-/Inhaltsfilter	Über ein Regelwerk definiert der Administrator, welche URLs und Inhalte blockiert werden sollen.
Intrusion Detection	Mittels Paket Inspection kann eine Abfolge von harmlosen Netzwerkpaketen als Eindringversuch erkannt werden.
Intrusion Prevention (NGFW)	Eindringversuche können durch Deep Paket Inspection (Nachrichtenanalyse) abgewehrt/verhindert werden. Diese Fähigkeit wird als Next Generation Firewall (NGFW) bezeichnet.

Technische Anforderungen an Firewalls	
Viren-, Spam-, Surfschutz	Eindringversuche finden über verschiedene Auslöser statt, z. B. per Phishing oder Malware. Aufgrund der o.a. Fähigkeiten ist der Auslöser irrelevant und ein Schutz über das Netzwerk wird gewährleistet.
DDoS Abwehr	Typische DDoS-Angriffe, z. B. ein massiver Empfang von unvollständigen Nachrichtenpaketen, werden erkannt und können abgewehrt werden.
Authentifizierung	Die Konfiguration der Firewall ist nur autorisierten Personen gestattet.
Quality of Service	Eine Priorisierung von IP-Paketen kann ebenso konfiguriert werden.
Reporting	Für den Administrator stehen Berichte zur Verfügung.
SFP/LAN/WIFI/LTE/UMTS	Entsprechend dem eingesetzten Netzwerk wird die Hardware Firewall ausgewählt.
Datendurchsatz	Der Datendurchsatz für Layer 3 Forwarding, Layer 5-7 Forwarding und die Anzahl maximaler gleichzeitiger Verbindungen sind entscheidende Kriterien.
VPN-/HTTP-Proxy	Als VPN-/HTTP-Proxy ist die Firewall in der Lage, auch den vertraulichen Datenverkehr zu scannen und filtern.
Bauform	Firewalls sind beispielsweise für 19-Zoll-Racks erhältlich oder auch als Stand- Alone-Geräte.
EU/EAA/NATO Restrict- ed/DSGVO	Für sicherheitsrelevante Bereiche gibt es Firewalls mit entsprechenden Zertifikaten.

Einfache Firewalls blockieren die ankommenden Pakete von IP-Adressen, die auf einer Sperrliste stehen (Blacklist). Oder sie akzeptieren die ankommenden Pakete der IP-Adressen, die auf der Liste erlaubter IPs stehen (Whitelist). Ein Beispiel für solch eine einfache Firewall ist die GNU Uncomplicated Firewall/Gufw für Linux Desktops (siehe nebenstehende Abbildung).

Firewalls werden über Regeln konfiguriert. Jede eingehende Nachricht wird gegen die Liste konfigurierter Regeln geprüft.

```

root@vmd51455:~# ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
5665/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
5665/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)

```

Als Beispiel einer Firewall-Konfiguration dient hier die Uncomplicated Firewall auf einem Linux-Server (siehe Abbildung links): Der Server bietet TCP- Dienste auf den Ports 22, 5665, 80 und 443 an, für IPv4 und IPv6.



Aufgrund des frei verfügbaren Quellcodes und der äußerst sensiblen Thematik „Abwehr von Angriffen von außen auf das eigene Netzwerk“ (Vermeidung von Industrie-Spionage) weichen Unternehmen auf Open- Source-Firewall-Lösungen aus.

Open-Source-Firewalls

IPFire

IPFire ist eine professionelle freie Firewall auf GPLv3-Basis von der Lightning Wire Labs GmbH aus Deutschland. Es besteht aus einem minimalistischen, gehärteten Betriebssystem mit Firewall und ist aufgrund der Größe hoch performant. Es teilt das Netzwerk in unterschiedliche Subnetze auf, z. B. LAN und DMZ, mit unterschiedlich anwendbaren Regeln. Es eignet sich für Intrusion Detection (IDS) und Intrusion Prevention (IPS), siehe <https://www.ipfire.org>.

OPNSense®

OPNSense ist eine Open-Source-Firewall auf FreeBSD-Lizenz der niederländischen Deciso und eine Abspaltung von pfSense®. Es unterstützt VPN, High Availability und Failover, IDS und IPS, DNS Server und Forwarder, DHCP Server, VLANs u. v m., siehe <https://opnsense.org>.

SecurityOnion

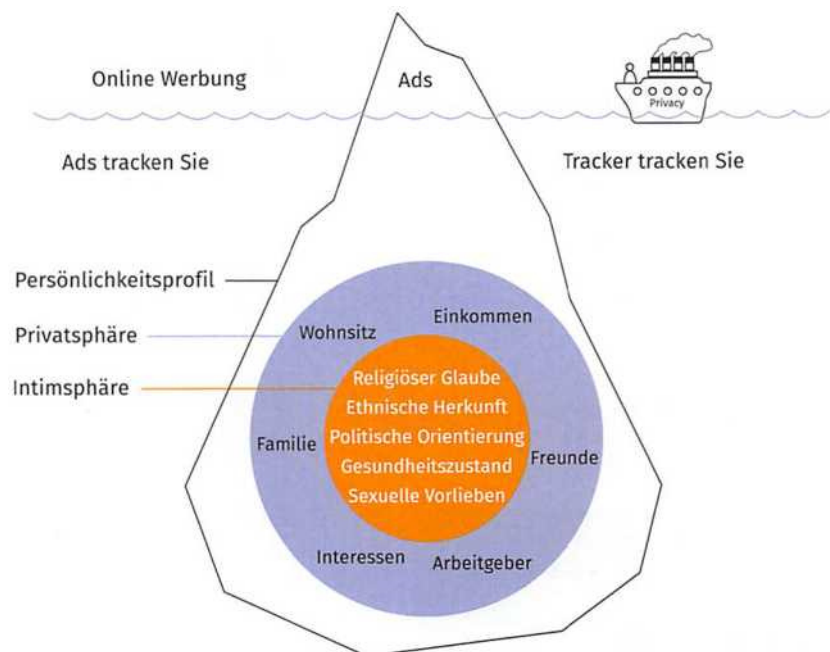
SecurityOnion ist eine Open Source Linux Distribution auf GPLv2 für Intrusion Detection, Network Security Monitoring und Log Management und ist als Container verfügbar. Das Projekt wird geleitet von der Security Onion Solutions, LLC, welche Hardware Appliances, Schulungen und Support anbietet, siehe <https://securityonionsolutions.com/software>.

Suricata

Suricata ist eine Thread Detection Engine und wird in Firewalls verwendet, z. B. IPFire, OPNSense® und SecurityOnion, siehe <https://suricata.io>.

LE 3 - DNS-Filter

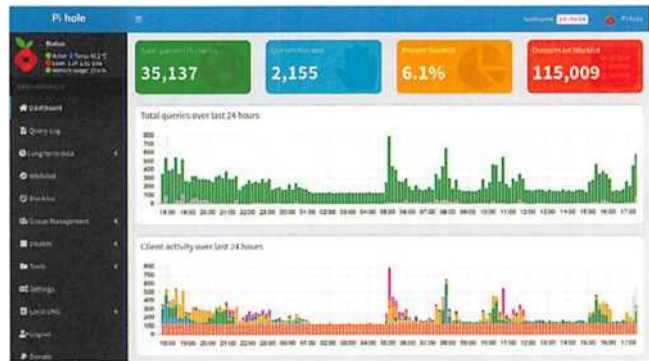
Bei DNS-Filtern handelt es sich um Software, welche Werbung, Tracker und Malware zentral in einem Netzwerk filtern kann. Das nebenstehende Schaubild zeigt, warum der Einsatz von DNS-Filtern sehr wichtig ist: Beim Surfen im Internet geben wir durch unser „Surfverhalten“ viel mehr über uns preis, als uns tatsächlich bewusst ist. Die Summe unseres gesamten Surfverhaltens gibt den Datensammlern ein sehr genaues Profil unserer Persönlichkeiten. Einen Schutz vor dieser „Sammelwut“ ermöglichen DNS-Filter.



Ein DNS-Filter muss 24 Stunden am Tag laufen, da er als DNS-Server agiert. Er wird daher oft in einer virtuellen Maschine oder auf einem separaten Rechner betrieben.

Der nebenstehende Screenshot zeigt die Weboberfläche eines Pi-Hole-Servers:

In dem aktiven Netzwerk wurden in den letzten 24 Stunden insgesamt 35137 DNS- Anfragen intern gestellt, davon 2155 gefiltert, dies entspricht 6,1 % aller DNS-Anfragen aus diesem Netzwerk.



DNS-Filter

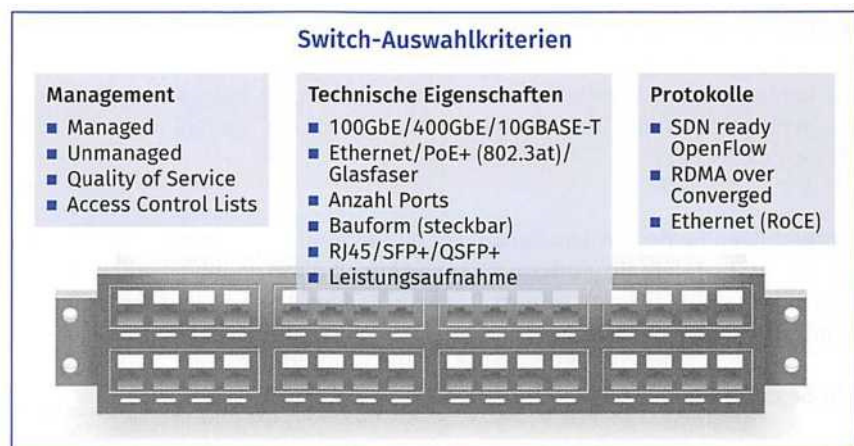
DNS-Filter werden logisch vor den eigentlichen DNS-Server im Netzwerk geschaltet. Sie entscheiden mittels sogenannter „schwarzer Listen“ (Black Lists), ob eine DNS-Anfrage zum eigentlichen DNS-Server weitergeleitet werden soll oder nicht (Filterfunktion). Diese Filterlisten müssen aber nicht von Hand gefüllt werden, sie können aus dem Internet von vertrauenswürdigen Anbietern bezogen werden. Professionelle DNS-Filter leiten die DNS-Anfragen zudem verschlüsselt weiter mittels DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNSCrypt oder DNS-over-QUIC (DoQ): Anfragen zum „eigentlichen“ DNS-Server im Internet können dann auf dem Transportweg weder verfolgt noch manipuliert werden.

Bekannte Open-Source-DNS-Filter sind „eBlocker“ (<https://eblocker.org>), „Pi-Hole“ (<https://pi-hole.net>) und „AdGuard“ (<https://adguard.com/de/adguard-home/overview.html>) zum zentralen Schutz ganzer Netzwerke vor Tracking und Werbung.

LE 4 - Switches

Switches sind Geräte, die Netzwerksegmente miteinander verbinden. Nachrichten werden an den Port weitergeleitet, an dem sich der Empfänger befindet.

Für Switches werden bei der Auswahl folgende Kriterien berücksichtigt:



Technische Anforderungen an Switches	
Managed Switches	Sie verfügen über eine integrierte Webanwendung. Über einen Browser lassen sie sich konfigurieren.
Unmanaged Switches	Sie sind fest konfiguriert, die Parameter sind nicht anpassbar.
Quality of Service	Mit QoS lässt sich der IP-Traffic per Konfiguration priorisieren.
Access Control Lists	Über ACLs lassen sich Zugriffsrechte festlegen.
100 GbE/40 GbE/ 10 GBase-T	Je höher die unterstützten Datendurchsatzraten sind, desto höher ist der Preis der Switches. Sehr hohe Datendurchsatzraten werden mit Glasfaser erreicht. Kleinere Durchsatzraten sind kostengünstiger.
Ethernet/PoE+/ Glasfaser	Switches sind unter Umständen mit unterschiedlichen Ports und Datendurchsatzraten in einem Gerät ausgestattet.

Technische Anforderungen an Switches	
Anzahl Ports	Die Anzahl an Ports ist ein weiteres wichtiges Kriterium.
Bauform	In Rechenzentren wird die 19-Zoll-Bauform bevorzugt mit ein, zwei oder mehreren Höheneinheiten (HE).
RJ45/SFP+/QSFP+	Über die Ports werden die Patchkabel (kurze Kabel) angeschlossen.
Leistungsaufnahme	Die Leistungsaufnahme wird in Watt pro Port angegeben.
Software Defined Networks	Diese Switches lassen sich in Software Defined Networks (SDN) konfigurieren und sind somit für Virtualisierte Rechenzentren geeignet.
RDMA over Converged Ethernet (RoCE)	Dieses Netzwerkprotokoll ermöglicht den direkten Speicherzugriff auf Switches über das Netzwerk. Damit lassen sich Latenzen im Netzwerk nochmals reduzieren und Datendurchsatzraten erhöhen.

LE 5 - VoIP-Telefonanlage

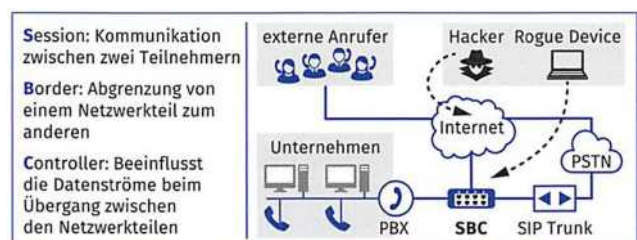
Mit der Umstellung der Telefonie von der Leitungsvermittlung auf das Internet-Protokoll sind VoIP-Telefonanlagen erhältlich. Sie können als Software, als virtuelle Maschine und als Hardware-Appliance bezogen werden. Auch bei Nutzung analoger oder ISDN-Endgeräte wird in Deutschland das Internet-Protokoll verwendet. Für den Verbindungsaufbau kommt das Session Initiation Protocol (SIP) zum Einsatz, für das eigentliche Gespräch das Transport Protocol for Real-Time Applications (RTP), siehe auch RFC3550 der Internet Engineering Task Force (IETF).

Bei der Umstellung auf eine VoIP-Telefonanlage ist darauf zu achten, ob bzw. wie die bereits vorhandenen Endgeräte weiter genutzt werden sollen bzw. können. Alternativ oder ergänzend dazu können sogenannte Softphones eingesetzt werden. Diese sind Programme, die auf den Rechnern installiert werden. Die Anwender nutzen dann zum Telefonieren ein Headset, welches am PC angeschlossen ist.

Unterstützen beide, das anrufende und das angerufene Endgerät, Zusatzfunktionen, z. B. Verschlüsselung und/oder HD-Telefonie (Codec G.722), so können diese genutzt werden. Die IP-Telefonie findet grundsätzlich unverschlüsselt statt. Unterstützen die Endgeräte keine Verschlüsselung, so kann ein Session Boarder Controller (siehe nächsten Abschnitt) diese Funktion übernehmen.

(1) Session Boarder Controller für VoIP

Ein Session Boarder Controller (SBC) ist eine Software zur Kopplung externer VoIP-Netze mit dem internen VoIP-Netz. SBC sind als Software und als dedizierte Hardware erhältlich.



Session Boarder Controller (SBC)

Interne Netze werden durch einen SBC gegen Angriffe über das SIP (Session Initiation Protocol) von außen geschützt. Ein SBC nimmt die Anrufe „entgegen“ und entscheidet anhand der empfangenen SIP-Pakete, ob und wie Gespräche mit internen Geräten oder Softphones aufgebaut werden sollen. SIP-Angriffe können zentral abgewehrt werden. Darüber hinaus lassen sich VoIP-Gespräche verschlüsseln (über TLS oder SRTP) und Protokolle übersetzen (SIP, H.323).

Technische Anforderungen an Session Boarder Controller (SBC)	
Anzahl gleichzeitiger Anrufe	SBC in Geräteform sind in ihrer Leistung begrenzt und können eine bestimmte Anzahl gleichzeitiger Anrufe handhaben.
Unterstützte Protokolle	Für die IP-Telefonie existieren eine Vielzahl an Protokollen, z. B. SIP, H.323, IAX (Inter Asterisk exchange).
RTP Transcoding	VoIP-Gespräche können technisch in unterschiedlichen Audio-Qualitäten durchgeführt werden. Beim Verbindungsaufbau wird der Audio-Codec ausgehandelt (G.711, G.722, G.729, etc.).
Fax Relay	Unterstützung des T.38-Standards für den Empfang von Fax.
SIP Intrusion Prevention	Eindringversuche über SIP werden erkannt und abgewehrt.
Schutz vor DDoS	DDoS-Angriffe über das Session Initiation Protocol werden erkannt und abgewehrt.
Gesprächssicherheit/Verschlüsselung	Die Gespräche finden über das Real-Time Transport Protocol (RTP) statt, siehe RFC3550 (https://datatracker.ietf.org/doc/html/rfc3550). Gespräche können, wenn es die Endgeräte unterstützen, mittels SRTP oder IPsec verschlüsselt werden.
Firewall	Eine interne Firewall leitet SIP-Anfragen weiter und wehrt alle anderen Anfragen ab.

LE 6 - Repeater

Repeater sind Signalverstärker. Sie empfangen ein (schwaches) Signal, bereiten es auf und senden es. Repeater werden sowohl bei Kupferkabeln als auch bei Glasfaser und WLAN eingesetzt, um die Reichweite zu erhöhen. Mithilfe von WLAN-Repeatern ist es beispielsweise möglich, ein WLAN-Signal über ein großes Firmengelände zu verteilen oder über große Entfernungen (mehrere Kilometer) von einem Ort zum anderen zu transportieren.

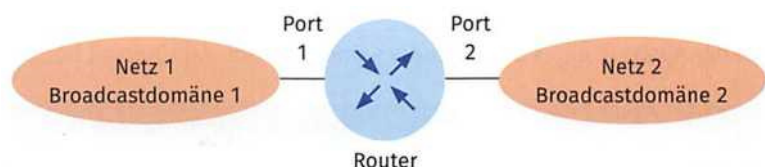


LE 7 - Router

Router leiten Datenpakete zwischen unterschiedlichen Netzwerken zum nächsten Router weiter. Sie verbinden Netzwerke und lenken den Datenverkehr mittels einer Routing-Tabelle.

Beispiel: Beim Aufruf einer Internetseite wird ein Datenpaket mit der Anfrage erzeugt. Dieses Paket wird vom anfragenden PC versendet, von Router zu Router durch das Internet geleitet und bis zum Zielservers transportiert. Die Adresse des Zielservers ist im Header der Nachricht angegeben. Der Zielservers nutzt nun die Absenderadresse des Headers als Zieladresse für die Antwort.

Router identifizieren ihre Ports (nicht zu verwechseln mit der Port-Nummer der IP-Nachrichten), ihre Netze und Broadcast-Domänen (alle Rechner, die bei einem Broadcast in diesem Subnetz erreicht werden), siehe nebenstehende Abbildung. Sie speichern alle Geräte, die bei einem Broadcast auf einem Port erreicht werden können. Befindet sich die Zieladresse nicht in den eigenen Netzen, so wird die Anfrage an den nächsten Router verschickt.

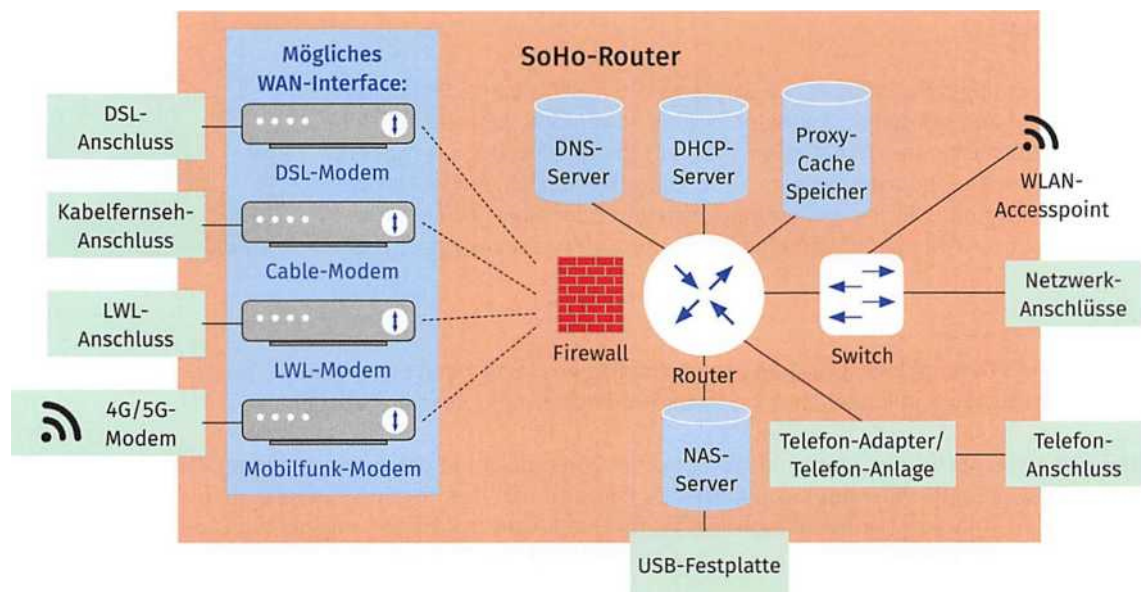


Router	
Heimrouter	Diese Route verbinden das Heimnetz mit dem Internet. Sie sind oftmals mit vielen weiteren Funktionen ausgestattet, z. B. Firewall, Access Point, Telefonanlage, Media-Server, Switch oder Jugendschutzfilter (siehe auch SoHo-Router)
Edge-Router	Edge-Router liefern eine deutlich höhere Performance als Heimrouter. Sie verbinden das Firmennetz mit dem Internet oder Partnernetz.
Core-Router	Core-Router sind höchst performante Router für Internet Service Provider (ISP). Diese Router erreichen ihre Performance u.a. dadurch, dass sie keine anderen Aufgaben übernehmen und per Glasfaser verkabelt sind.
Virtuelle Router	Virtuelle Router finden in Software Defined WANs Verwendung.

Der Einsatzbereich legt fest, für welche Netze und welche Performance ein Router ausgelegt werden muss.

Heimrouter (SoHo-Router)

Sogenannte SoHo-Router, SoHo steht für Small Office - Homeoffice, sind kleine leistungsfähige All-in-one-Router. Sie verfügen über eine Vielzahl unterschiedlicher Gateways, Serverdienste und Anschlüsse. Zudem sind sie mit einem oder mehreren WAN Interfaces/Schnittstellen ausgestattet. Das folgende Schaubild zeigt, dass die Hersteller von SoHo-Routern viele Funktionen unterbringen.



Bei der Auswahl eines SoHo-Routers sind folgende Kriterien zu berücksichtigen:

Kriterien für SoHo-Router	
WAN- Interface(s)	Viele SoHo-Router besitzen genau ein WAN-Interface, z. B. DSL oder Kabel-TV oder LTE oder Glasfaser. Einige Hersteller bieten Router mit mehreren WAN-Interfaces: Damit wäre das Internet auch dann verfügbar, wenn ein WAN-Interface ausfällt. Besitzt der Router USB-Anschlüsse, so ist zu prüfen, ob sich mittels eines USB- LTE-Sticks ein LTE-WAN nachrüsten lässt.
DNS-Server	Router nehmen die DNS-Fragen des Netzwerks entgegen. Idealerweise lässt sich die Adresse des DNS-Servers auch konfigurieren, um z. B. einen DNS-Filter im Netzwerk zu integrieren.

Kriterien für SoHo-Router	
DHCP-Server	Ein interner DHCP-Server erlaubt die dynamische IP-Adressvergabe. Idealerweise lässt sich der zu vergebende Adresspool konfigurieren, um auch statische IP-Adressen vergeben zu können. Diese sind oft erforderlich für Server im Netzwerk.
Proxy Server	Einmal aus dem Internet geladene statische Webseiten können beim nächsten Aufruf aus dem Cache des Routers geliefert werden. Proxys reduzieren den Datenverbrauch und sind sinnvoll bei Volumentarifen.
WLAN-Access-Point	Beim WLAN-Access-Point ist es hilfreich, wenn ein zusätzliches Gastnetz genutzt werden kann und eine nächtliche Abschaltung des WLANs möglich ist.
Kindersicherung und Jugendschutzfilter	Da die Heimrouter auch in Familien eingesetzt werden, sind eine Kindersicherung, die Unterstützung von Zeitkontingenten und Jugendschutzfilter hilfreich.
Anzahl Ethernet Ports	Um den Kauf eines zusätzlichen Switches zu vermeiden, sollte der Router über ausreichend (Gigabit)-Ethernet-Anschlüsse verfügen.
TK-Anlage	Eine integrierte Telefonanlage und entsprechende Anschlüsse sind erforderlich, wenn bereits vorhandene Analog- und ISDN-Haustelefone weitergenutzt werden sollen.
NAS-Server	Ein integrierter NAS-Server kann durch Anschluss eines USB-Laufwerks genutzt werden. Der USB-Anschluss sollte mindestens USB 3.0 unterstützen, wenn der integrierte NAS-Server zur Sicherung genutzt werden soll.

Router verfügen intern über einen Webserver, hierüber wird eine Weboberfläche zur Konfiguration bereitgestellt. Eine Open-Source-Router-Alternative ist „OpenWrt“ (<https://openwrt.org>). Es unterstützt viele WLAN-Router (<https://openwrt.org/toh/start>) und lässt sich über ein Paketmanagement erweitern.

Edge- und Core-Router

Folgende Kriterien sind bei der Auswahl von Unternehmens-/Edge- und High-Performance-/Core- Routern relevant:



Technische Anforderungen an Router	
Anzahl 10/100/1000/10G/100G/400G Ports	Je nach Einsatzbereich (Heim, Edge, Core) finden sich entsprechende Router mit 10, 100, 1000 MBit/s oder bis zu 400 Gbit/s Ports.
Anzahl QSFP56/ QSFP28/ SFP/SFP+/RJ45 Ports	Je mehr Ports zur Verfügung stehen, umso mehr Netzwerke lassen sich anschließen. Modulare Transceiver (Sender/Empfänger-Module, siehe Abbildung) unterstützen die Spezifikation „Small Form-Factor Pluggable“. Darüber kann ein Router mit optischen oder elektrischen Transceivern via Plug and Play zu den bereits vorhandenen RJ45-Ports nachgerüstet werden. Die maximale Datenrate bei QSFP56-Transceivern beträgt 50 Gbit/s, bei QSFP28 Transceivern 25 Gbit/s.
IPsec	Router mit IPsec können als VPN-Router eingesetzt werden.
Software defined WAN	Die Routing-Regeln lassen sich per Konfiguration festlegen.
CPU/RAM	Auch bei Routern gilt: Möglichst viele Rechenkerne mit hoher Single-Thread- Leistung und viel RAM bedeuten eine bessere Gesamtperformance.
M.2-Storage-Größe	Der M.2-Storage wird für das lokale Logging verwendet.
Anzahl IPsec-Tunnel	Dieser Wert gibt an, wie viele Standorte ein Unternehmen mit diesem Router anbinden kann.
SD-WAN-IPsec-Durchsatz	Der SD-WAN-IPsec-Durchsatz ist entscheidend für Unternehmen, die ihre Standorte mittels IPsec-Tunnel verbinden wollen.
Dualpower/PoE	Dual-Power Geräte laufen auch dann, wenn eine Stromversorgung ausfällt. Dualpower bedeutet eine höhere Ausfallsicherheit. Die „zweite“ Stromversorgung erfolgt über Power over Ethernet. PoE und PoE+ (802.3af/at) erfordern unterschiedliche Leistungen.
Anzahl Höheneinheiten	Core- und Edge-Router sind für 19-Zoll-Racks ausgelegt.
Management Cloud	Der Router-Hersteller stellt eine Cloud-Anwendung bereit, über die der Kunde alle seine Netzwerkkomponenten dieses Herstellers zentral konfigurieren und überwachen kann.

LE 8 - Gateway

Gateway ist ein Oberbegriff für Netzwerkkomponenten, die eine Verbindung zwischen zwei Netzen herstellen. Je nach ISO/OSI Layer finden sich hier folgende Netzwerkkomponenten:

Gateways	
Hub	Hubs arbeiten auf dem ISO/OSI Layer 1 als Verteiler von Netzwerkdaten. Sie empfangen Daten und senden diese an alle Ports.

Gateways	
Bridge	Eine Bridge verbindet Netzwerksegmente auf ISO/OSI Layer 2. Sie werden eingesetzt, um z.B. Netze in mehrere Kollisionsdomänen aufzuteilen. Da alle Netzwerkkarten mit dem CSMA/CD-Verfahren arbeiten, sollte die Kommunikationslast aller Geräte nicht zu hoch sein. Anderenfalls müssen einzelne Komponenten mit dem Senden zu lange warten.
PowerLAN	PowerLAN bzw. Powerline Adapter verwenden die vorhandenen elektrischen 230-V-Leitungen eines Gebäudes zur Datenübertragung. Die Nutzdaten werden über ein Trägersignal aufmoduliert. So lässt sich das Intranet nachträglich in Räume „bringen“, die nicht mit Netzwerkdosen verkabelt sind. Es werden mindestens zwei Powerline-Adapter benötigt, ein Anfangspunkt und ein Endpunkt. Wichtig: Je länger die Stromleitung ist und je mehr Verteiler zwischen Anfangs- und Endpunkt liegen, umso größer ist die Dämpfung. Powerline-Adapter arbeiten auf der OSI-Schicht 1. Bei der Auswahl ist zu berücksichtigen, dass die eingesetzten Adapter möglichst vom gleichen Hersteller sein sollten. Je nach Hersteller können theoretische Übertragungsraten von bis zu 1 200 MBit/s erreicht werden. Einige Adapter sind in der Lage, zusätzlich ein WLAN-Access Point bereitzustellen. 
Layer 3 Gateways	Layer 3 Gateways werden auch als Router bezeichnet. Sie stellen eine Verbindung zwischen Subnetzen her. LTE-Router stellen ein lokales Netz (WLAN) bereit und verbinden dieses mit dem 4G-LTE-Netz. LTE-Router gibt es u.a. für den mobilen Einsatz (siehe Abbildung). 
NAT Gateways	NAT Gateways übernehmen die Aufgabe der Network Address Translation bei IPv4-Netzwerken.
TLS Gateway	Die Terminierung von TLS-Verbindungen ist ein Beispiel für Layer 4 Gateways. So kann z.B. eine Firewall diese Aufgabe übernehmen.
Proxy	Gateways auf den OSI Layern 5-7 werden als Proxy oder Application Layer Gateway bezeichnet. Sie empfangen Nachrichten als Stellvertreter, analysieren diese und leiten sie ggf. weiter an den eigentlichen Server. Bekannte Proxy-Server sind SIP-, FTP-, E-Mail- und http-Proxy. Diese werden als Sicherheitskomponente für Anfragen aus dem Internet in der Demilitarized Zone (DMZ) zwischengeschaltet.
VPN Gateways	VPN Gateways erlauben einen sicheren Zugriff auf das Firmennetz. Dazu wird im Firmennetz ein VPN-Server bereitgestellt, z. B. als Teil einer Firewall oder eines Routers oder als Open Source Server, z. B. WireGuard (https://www.wireguard.com).

TAG 6 - Server-Software unterscheiden

Verschiedene Möglichkeiten der Virtualisierung sind heute verfügbar. Da unter dem Marketingnamen „Cloud“ die Virtualisierung ganzer Rechenzentren voranschreitet, geht dieses Kapitel auf die Virtualisierungstechniken ein und ein späteres Kapitel auf die Server-Hardware und Produkte.

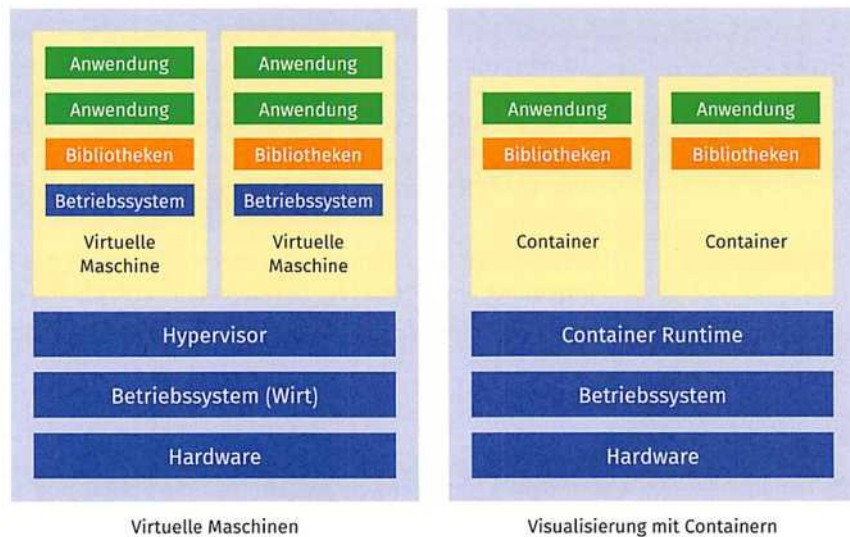
LE 1 - Server-Virtualisierung mittels virtueller Maschinen und Containern

Mit der Virtualisierung von Servern entfällt die Abhängigkeit von der darunterliegenden Hardware. Sie wird austauschbar. Virtualisierung bietet zudem den Vorteil, dass die erforderlichen Ressourcen wie CPU- Kerne und Speicher beliebig skaliert werden können. Mehrere Virtualisierte Server (auch VM, virtuelle Maschine) können dadurch auf einer Hardware laufen.

Bei der Überprovisionierung werden mehr virtuelle CPU-Kerne an virtuelle Maschinen verteilt, als physikalisch vorhanden sind. Dies führt ggf. dazu, dass einer virtuellen Maschine CPU-Zeit „gestohlen“ wird, weil eine andere VM gerade unter Volllast läuft.

Container werden als leichtgewichtige virtuelle Maschinen bezeichnet. Gegenüber VMs wird auf ein eigenes Betriebssystem verzichtet - sie nutzen das Betriebssystem des Wirts. Ein Container enthält die Binärdaten, also die Anwendung inklusive aller erforderlichen Bibliotheken.

Beispiele für Container sind Docker, CRI-O oder Kata Containers. Mit Containern lässt sich über eine entsprechende Orchestrierungsplattform, z. B. Kubernetes, hoch skalierbare Server-Software betreiben.



Unterschiede zwischen virtuellen Maschinen und Containern	
Virtuelle Maschine	Container
- Bei einer virtuellen Maschine läuft ein Betriebssystem mit Anwendungen auf einer emulierten Hardware. - Betriebssystem und Anwendungen laufen in einer isolierten Umgebung. Sie können nur auf die ihnen zugeteilten Ressourcen zugreifen. - Mehrere virtuelle Maschinen können parallel auf einem Computer gestartet werden: Grenzen sind die Ressourcen der Hardware. - Ein Hypervisor betreibt die VMs.	- Bei Containern wird ein Prozess isoliert, z. B. eine Datenbank oder ein Webserver. - Container nutzen das Betriebssystem des Wirts. - Mehrere Container können parallel laufen. Grenzen sind die Ressourcen der Hardware/VM. - Eine Containerumgebung betreibt die Container. - Da die Container die Ressourcen des Wirt-Systems nutzen, werden weniger CPU-, Speicher- und Festplattenressourcen genutzt.

Hypervisor

Ein Hypervisor kommt bei virtuellen Maschinen zum Einsatz. Hierbei handelt es sich um eine Software, welche die Computerhardware emuliert und somit die parallele Installation mehrerer Betriebssysteme ermöglicht.

Hypervisor	
Hypervisor Typ 1 (Bare Metal)	Hypervisor Typ 2 (Hosted)
- läuft direkt auf der Hardware <i>Beispiele:</i> „VMware ESXi“ und der Open-Source- Hypervisor „Xen Next Generation“ (XCP-NG)	- läuft auf einem Betriebssystem - Gastsystem läuft als Prozess auf dem Wirt <i>Beispiele:</i> „Proxmox VE“ und „VMware Player“

Mit einer entsprechenden Verwaltungssoftware lassen sich virtuelle Maschinen und Container administrieren. Beispiele für solche Verwaltungssoftware sind die Open Source „oVirt“ mit KVM-Hypervisor (<https://www.ovirt.org>), der Sovereign Cloud Stack der europäischen Gaia-X Initiative oder das kommerzielle „VMware vSphere“.

Das folgende Bild zeigt die Weboberfläche zur Administration einer virtuellen Maschine mit zwei Snapshots. Im Beispiel wurden die Snapshots mit der Bezeichnung „debian 10“ und „Open Nebula ready“ erstellt.



Für die Administration virtueller Maschinen sind u.a. folgende Funktionen über den Browser durchführbar:

Administration virtueller Maschinen	
Szenario	Beschreibung
Snapshots	Snapshots können erstellt werden, um den aktuellen Zustand des (laufenden) Systems zu sichern. Sollten anschließende Updates, z. B. der Datenbank, fehlschlagen, so genügt ein Klick auf Rollback, um den Zustand vor dem Update wiederherzustellen. Bei Copy-on-Write-Verfahren dauert die Erstellung genau einen Mausklick.
Start & Stop	Zum Starten und Stoppen virtueller Server und Container genügt ein Klick in der entsprechenden Management-Software im Browser. Ist diese Management-Software im Internet verfügbar, so können das Starten und Stoppen von überall auf der Welt erfolgen.
Neustart	Hierüber lässt sich die virtuelle Maschine booten.
Rollback	Snapshots lassen sich über Rollback zurückspielen.

Vor- und Nachteile von Virtualisierung	
Vorteile	Nachteile
• Unabhängigkeit von der Server-Hardware: Durch die Nutzung Virtualisierter Hardware bleibt diese immer gleich - auch wenn sich die physikalische Hardware ändert. • Serverkonsolidierung: Mehrere physikalische Server können als VMs auf einer Serverhardware installiert werden. Dies spart Energie und Platz. • Höhere Verfügbarkeit: Weniger Hardware bedeutet weniger Ausfall. • Schnelle Bereitstellung: Virtuelle Ressourcen sind deutlich schneller verfügbar als Hardware-Ressourcen. • Ressourcenengpässe können per Konfiguration im laufenden Betrieb behoben werden.	• Know-how erforderlich: Während die Inbetriebnahme physikalischer Geräte sehr anschaulich ist, müssen sich Cloud-Administratoren „neu“ in die Konfiguration virtueller Rechenzentren einarbeiten. Jede Cloud-Software, jeder VM-Typ und Container-Typ besitzt seine eigenen Werkzeuge. • Single Point of Failure: Wird ein einziges Bare Metal benutzt, dann fallen bei Ausfall dieser Hardware alle virtuellen Maschinen aus. Cluster sollten daher über mehrere Bare Metals verteilt laufen.

Beispiele für Virtualisierungsplattformen

Virtualisierung kommt heute überall zum Einsatz. Sie ermöglicht eine optimale Auslastung der Hardware, dadurch geringere Betriebskosten, eine einheitliche Handhabung von Ausfällen (Failover) und bessere Sicherheitskonzepte. Beispiele für Virtualisierungsplattformen sind „Kernel based Virtual Machine“ (KVM), „OpenVZ“, „Microsoft's Hyper-V“, „Parallel's Desktop for Mac“, „QEMU“, „VirtualBox“, „VMware Fusion“ und Server, „XEN Server“.

Beispiel für einheitliches Failover

Mindestens zwei Bare Metals und ein RAID6- oder RAID10-Verbund stellen sicher, dass bei Ausfall einer Hardware alle VMs weiterlaufen bzw. ausgefallene VMs nachgestartet werden. Um den Ausfall eines ganzen Rechenzentrums zu kompensieren, kann eine entsprechende Cloud-Software über mehrere Rechenzentren hinweg eingesetzt werden. Welche Anwendung in welcher VM läuft, ist bei Ausfall einer Festplatte, CPU, eines Speichers oder einer Netzwerkkarte unerheblich.

LE 2 - Software as a Service (SaaS)

SaaS beschreibt eine Mietlösung, bei der der Anbieter die Anwendungssoftware auf einem Server bereitstellt. Beispiele hierfür sind „Trello“, „Salesforce“ und „Microsofts Office 365“.

Vor- und Nachteile von SaaS	
Vorteile	Nachteile
• Mitarbeiter des Kunden erhalten weltweiten Zugriff über Browser • der Kunde muss keine Server-IT bereitstellen • der Kunde muss sich nicht mit Hardware, Betriebssystem, Datenbanken, Firewalls etc. auseinandersetzen • die Lösung skaliert mit dem Bedarf des Kunden • keine Aufwände bezüglich Wartung der Lösung	• der Kunde ist abhängig vom Dienstleister • der Kunde erhält einen „Standard“, wie ihn der Anbieter definiert • benötigte Schnittstellen zu Drittsystemen sind ggf. nicht vorhanden • der Anbieter erhält einen einfachen Zugriff auf die Kundendaten und somit ggf. Zugriff auf die Daten ganzer Branchen • großes Vertrauen und klare vertragliche Regelungen erforderlich

LE 3 - Webhosting

Webhosting ist eine besondere Form des SaaS. Der Kunde erhält hierbei eine browserbasierte Administrationsoberfläche für die One-Click-Installation von Server-Anwendungen.

Webhosting-Software erlaubt das Installieren und Konfigurieren von Webanwendungen über einen Browser. Mit dem Webhosting Control Panel können Domains, Sub-Domains und E-Mail-Adressen konfiguriert werden. Sie erlauben zudem das Sichern, Wiederherstellen und Staging (das Arbeiten mit einer Kopie) von Webanwendungen. Beispiele sind „cPanel“ (<https://cpanel.net>), „Plesk“ (www.plesk.com) und „CentOS Webpanel“ (<http://centos-webpanel.com>)

Webhosting Control Panel

Bei einem Webhosting Control Panel handelt es sich um eine Software as a Service, bei der der Kunde eine Administrationsoberfläche für Webanwendungen erhält. Diese Produkte werden alternativ auch als Shared Hosting oder Webspace bezeichnet.

Viele Webanwendungen benötigen eine Datenbank, z. B. MySQL, und einen Webserver, z. B. apache2. Beim Webhosting stellt der Provider dem Kunden eine Hosting-Anwendung, z. B. „plesk“, „cPanel“, „interworX“, „DirectAdmin“, zur Verfügung. Darüber kann der Kunde seine Server-Anwendungen installieren, administrieren und aktualisieren. Technisch betrachtet teilen sich alle Kunden eine MySQL Datenbank und ein Dateisystem: Jeder Kunde wird als „virtueller Host“ des Apache/-Webserver abgebildet. Der Kunde kann E-Mail-Adressen und -Weiterleitungen einrichten, Domänen und Subdomänen konfigurieren, Zugriffsstatistiken einsehen, den Server mittels IP-Black-Lists, SSL und 2FA absichern und vieles mehr.

Über die kommerzielle Erweiterung „Softaculous“ lassen sich mit wenigen Mausklicks weitere Webanwendungen, z. B. „Wordpress“, „Joomla“, „Mautic“, „Nextcloud“, „Shopware“ oder „SugarCRM“ installieren und konfigurieren.

Technische Anforderungen an Webhosting Control Panel	
Shared Host/ eigener VPS	Bei einem Shared Host liegen die eigenen Daten mit denen anderer Kunden auf demselben Host. Nach Möglichkeit sollte das Control Panel auf einem eigenen VPS/VDS installiert werden (Datenhoheit verbleibt beim Kunden).
Speicher	Kleinere Pakete bieten 50 GB SSD-Speicherplatz, größere bis zu 1 TB SSD-Speicherplatz. Neuere Server bieten NVMe-Speicherplatz, ältere Server HDD.
Anzahl DB	Die maximale Anzahl Datenbanken entspricht der maximalen Anzahl installierbarer Webanwendungen.
DB-Webzugriff	Ein Zugriff auf die Datenbanken der Webanwendungen wird per Browser ermöglicht.
Auto-Installer	Über einen integrierten Auto-Installer, z. B. „Softaculous“, kann der Kunde weitere Webanwendungen aus den Bereichen Blog, Forum, E-Commerce, ERP, Shop, Wiki in Subdomains installieren.
Anzahl Domains	Eine Domain ist oft inbegriffen. Sollen mehr Domains abgebildet werden, so ist ein größeres Paket zu wählen.
Anzahl Subdomains	In kleineren Paketen sind 100 Subdomains inbegriffen, in größeren Paketen bis zu 1000 Subdomains.
SSL-Zertifikate	Bei den im Angebot erwähnten SSL-Zertifikaten handelt es sich oft um kostenpflichtige Zertifikate, z. B. „Symantec Basis SSL“, die inbegriffen sind. Let's-Encrypt-Zertifikate werden separat erwähnt.

Technische Anforderungen an Webhosting Control Panel	
Anzahl E-Mail-Adressen	Entsprechend der Anzahl Mitarbeiter des Kundenunternehmens sollte ein Paket mit ausreichender Anzahl an E-Mail-Adressen gewählt werden. Der Zugriff auf die E-Mails erfolgt wahlweise über Webmail, IMAP, SMTP, POP.
FTPS/SSH- Zugang	Einige Webanwendungen erfordern einen FTPS und/oder einen SSH-Zugang, um Konfigurationen und/oder Updates durchführen zu können. Grundsätzlich ist es sinnvoll, einen SSH-Zugang zu besitzen, z. B. zur Ausführung von Reparaturskripten.
DNSSEC	Die abhörsichere DNS-Variante „DNSSEC“ ist bei immer mehr Providern bestellbar. Die Verfügbarkeit hängt von der Top Level Domain ab.
Konfigurierbare DNS Records	Domains und Subdomains konfiguriert der Kunde selbst. Dabei stehen die DNS- Felder A, AAAA, MX, CNAME, TXT, SRV und NS zur Verfügung.
DDoS-Schutz	Alle Webanwendungen werden vor Distributed-Denial-Of-Service-Angriffen (DDoS-Angriffen) geschützt.
Traffic	Unbegrenzter Traffic bedeutet, dass keine weiteren Kosten dafür anfallen.
IPv6-Adresse	Der Kunde erhält eine IPv6-Adresse.
Anzahl Cron-Jobs	Jede Webanwendung benötigt einen Cron-Job. Die Anzahl Cron-Jobs sollte daher mindestens der Anzahl Datenbanken entsprechen.
PHP, Python, NodeJS, Ruby	Einige Webanwendungen benötigen zusätzlich PHP, Python, NodeJS oder Ruby on Rails. Die Voraussetzungen der zu installierenden Webanwendungen sollten vorab geprüft und erst <u>danach</u> der Provider gewählt werden.
PHP-Version und PHP-Parameter	Einige Provider erlauben die Konfiguration wesentlicher PHP-Parameter wie Memory Limit, Upload Filesize, Execution Time, PHP-Version, Fast-CGI, Opcode- Cache etc. Auch hier ist vor der Provider-Wahl zu prüfen, inwieweit die zu installierenden Webanwendungen Anpassungen benötigen.
Back-up	Können Backups von den Webanwendungen mit dem Control Panel erstellt werden? Können Backup (externe) Storage konfiguriert werden?
Verfügbarkeit	Webhosting Control Panel können ggf. auch auf einem eigenen VPS, VDS oder dediziertem Server installiert und lizenziert werden. Damit erhält der Kunde ein eigenes, nicht mit anderen Kunden geteiltes System.
Laufzeit	Laufzeiten von sechs Monaten oder zwölf Monaten sind üblich.
Kosten	Übliche Kosten sind monatliche Kosten zzgl. einer einmaligen Einrichtungspauschale.

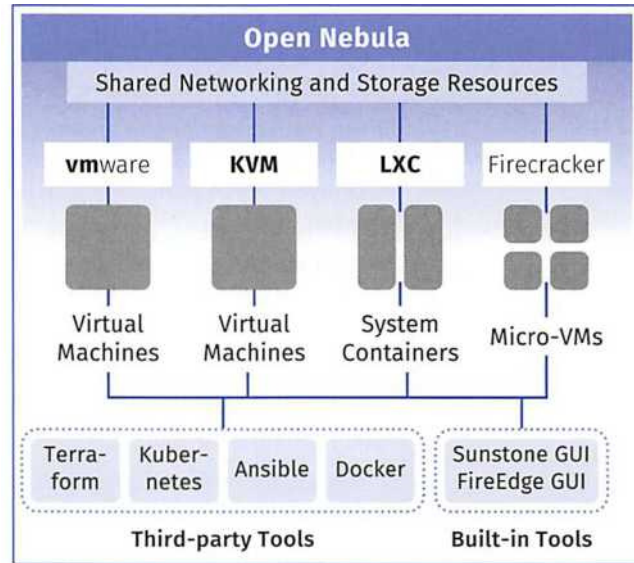
LE 4 - Infrastructure as a Service (IaaS)

Für den Betrieb von hyperkonvergenten Rechenzentren werden kommerzielle Produkte wie „VMware“ oder „XEN“ eingesetzt.

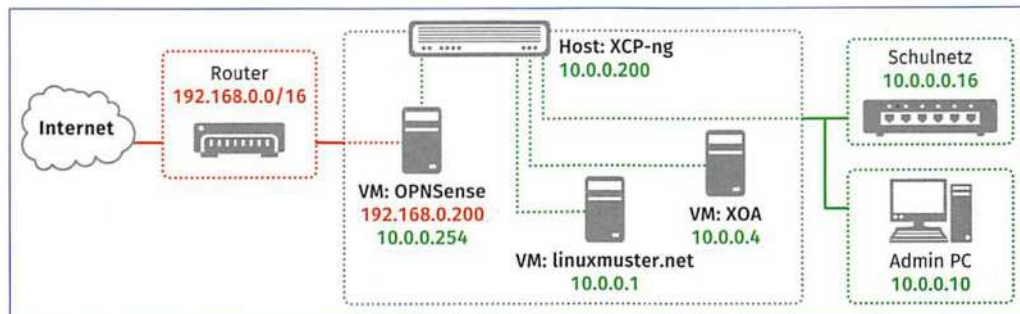
Bei einer hyperkonvergenten Infrastruktur wird das gesamte (verteilte) Rechenzentrum inklusive aller Prozessoren, Speicher (SAN, NAS), Netzwerke und Virtualisierung über eine einzige Administrationsoberfläche gesteuert.

Aufgrund sehr hoher Lizenzkosten kommen vermehrt Open-Source-Lösungen wie „Proxmox“ (<https://pve.proxmox.com>), „OpenNebula“ (<https://opennebula.io>) und „XCP-NG“ (<https://xcp-ng.org/>) zum Einsatz.

Das Schaubild gibt eine Übersicht zur EU- geförderten Plattform „Open Nebula“: Die Plattform unterstützt die Ausführung von Containern und virtuellen Maschinen und Technologien wie VMware, KVM, LXC und Firecracker Micro-VMs.



„XCP-ng“ ist eine Open-Source-Cloud-Plattform mit vielen Enterprise-Funktionen. Sie kann z. B. für Schulnetze eingesetzt werden (siehe Abbildung auf nächster Seite): Bei „linuxmuster“ (<https://www.linuxmuster.net>) handelt es sich um eine umfassende Komplettlösung für den Betrieb schulischer Netzwerke, welche sich auf einen „XCP-ng“- Host betreiben lässt. Die Plattform wird von Lehrkräften und Dienstleistern für die speziellen Anforderungen in der Schule entwickelt, ihre Pflege von einem gemeinnützigen Verein organisiert. „linuxmuster.net“ lässt sich ebenso auf „Proxmox“ oder „OpenNebula“ betreiben.



Technische Anforderungen an Server-/Rechenzentrumssoftware	
Hyperkonvergentes Rechenzentrum	Es bedeutet, dass bei Einsatz dieser Software jede Komponente ausfallen darf. Mittels räumlich verteilter Storage-Lösungen, z. B. CEPH (massiv skalierbares verteiltes Speicher- und Dateisystem, „SAN als Software“), erhalten die VMs weiterhin Zugriff auf Storage.
Webkonsole	Virtuelle Maschinen lassen sich über eine Webanwendung administrieren.
Paravirtualisierung	Bei der Paravirtualisierung werden in den virtuellen Maschinen (VMs) IO-Treiber installiert. Die VMs laufen performanter, weil sie direkt auf die physikalische Hardware, z. B. die GPU der Grafikkarte, zugreifen können.
Live-Migration	Virtuelle Maschinen lassen sich im laufenden Betrieb auf andere Knoten bzw. andere Hardware verschieben.
Orchestrierung	Management von Multi-Cluster-Container-Umgebungen; Unterstützung von virtuellen Maschinen, Containern, Kubernetes
VM-Hochverfügbarkeit	Virtuelle Maschinen werden bei Ausfall automatisch nachgestartet.
Back-ups	Periodisches Sichern von Daten der VMs auf remote Storage

Technische Anforderungen an Server-/Rechenzentrumssoftware	
ACLs	Zugriffssteuerung über Access-Control-Listen
Aufgabenplanung	Ein Planungsmodul erlaubt das zeitgesteuerte Ausführen von Aufträgen.
2FU	Logins lassen sich über Zwei-Faktor Autorisierung schützen.

Managed Hosting

Beim Managed Hosting übernimmt der Provider das Einrichten und die Wartung des Kundenservers. Der Kunde entscheidet sich für ein Hosting-Paket (VPS, VDS, Dedicated Server, Webhosting) und die einzurichtende Serversoftware.

Betriebssysteme

Betriebssysteme spielen im Serverbereich eine immer geringere Rolle. Sie sollen den Anwendungen nur noch die Ressourcen zur Verfügung stellen, die sie tatsächlich benötigen. Die Devise lautet: Betriebssysteme müssen so schlank wie möglich und nur so groß wie nötig sein, denn je kleiner das Betriebssystem ist, umso weniger Speicher benötigt es, umso performanter läuft es und umso kleiner ist die Angriffsfläche für Schadsoftware. Alle nicht benötigten Dienste eines Servers werden daher abgeschaltet und deinstalliert. Am einfachsten lassen sich diese Paradigmen mit Open-Source-Betriebssystemen umsetzen, z.B. "Debian", „CentOS“, „Ubuntu“, „Fedora“ (siehe auch <https://distrowatch.com>).



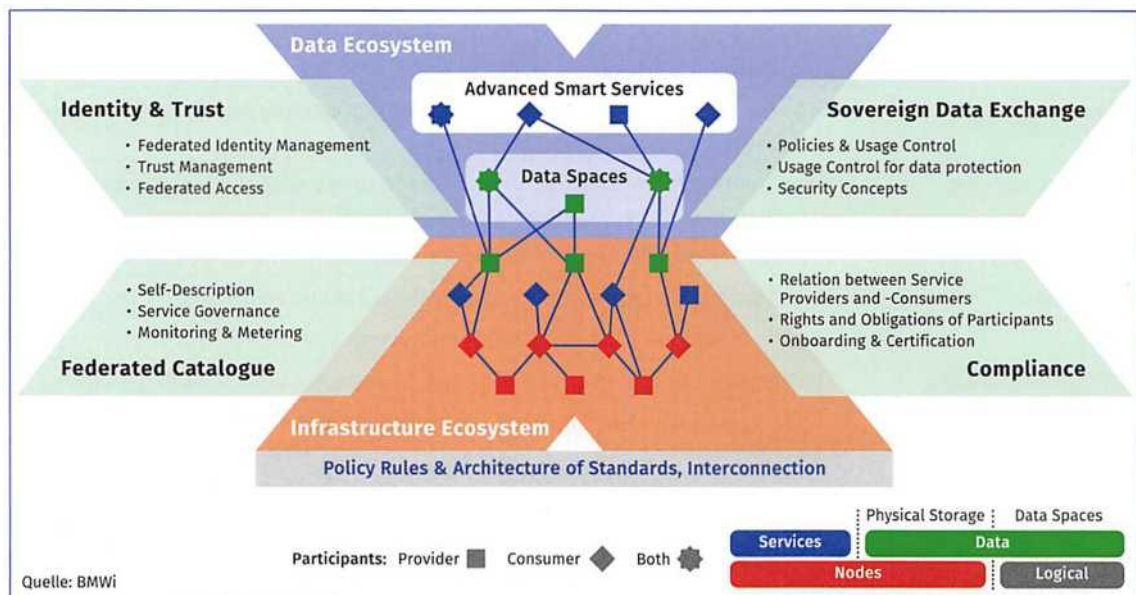
Mit dem Konzept der Container wurde das o.a. Paradigma auf die Spitze getrieben: Container erhalten nur die Ressourcen, die sie tatsächlich benötigen. Container werden daher auch als leichtgewichtige virtuelle Maschinen bezeichnet.

Ausblick: GAIA-X

GAIA-X ist ein Projekt Europas zum Aufbau einer europäischen Dateninfrastruktur. Oberstes Ziel dabei ist die Gewährleistung des Datenschutzes auf allen Ebenen.

GAIA-X Architektur Richtlinien	
Security by Design	Sicherheitsaspekte haben die höchste Priorität bei Design und Implementierung.
Privacy by Design	Datenschutzaspekte haben die höchste Priorität bei Design und Implementierung.
Enabling Federation, distribution and decentralisation	Verteilung, Dezentralisierung und Föderation, also das Zusammenspiel der verteilten Architektur, gehört ebenso zur höchsten Priorität.

Aus Architektursicht soll dies erreicht werden über sogenannte föderierte Dienste. Diese stellen die Laufzeitumgebungen für Gaia-X Anwendungen dar. Dazu zählen beispielsweise souveräne Datendienste, welche die Identitäten von Sender und Empfänger sicherstellen und ebenso die Nutzungsrechte auf Daten.



Das Projekt wird finanziell vom Bundesministerium für Wirtschaft und Energie bis Herbst 2022 unterstützt. Weitere Infos zu GAIA-X finden sich unter www.data-infrastructure.eu.

TAG 7 - Server-Hardware unterscheiden

LE 1 - Dedicated Server/Bare Metal

Bei einem Dedicated Server kauft oder mietet der Kunde bei einem Provider/Hoster einen physikalischen Server, einen sogenannten Bare Metal, welcher bei Miete oder Co-Location im 19-Zoll-Rack des Hosters verbleibt. Dedicated Server eignen sich für Anwendungen, bei denen der Kunde sicherstellen möchte, dass diese Hardware ausschließlich durch ihn genutzt wird.

Folgende Kriterien sind bei der Auswahl zu berücksichtigen:

Technische Anforderungen an Dedicated Server	
CPU und Anzahl Kerne	CPUs sind üblicherweise Intel XEON, AMD EPYC oder AMD Ryzen mit bis zu 32 Rechenkernen (Cores).
Speicher	RAM ist erhältlich von 256 GB ECC (Error Correction Code) bis zu 2 TB. ECC-Speicher ist in der Lage, Bit-Fehler zur Laufzeit zu reparieren.
Anzahl IPv4-/IPv6-Adressen/ Failover IP	Je eine IPv4- und IPv6-Adresse sind oftmals inklusive. Weitere öffentliche IP-Adressen können dazu gebucht werden. Mittels einer Failover-IP ist der Server auch dann erreichbar, wenn die andere IP-Adresse/Netzwerkkarte ausfallen sollte.
Reverse-DNS	Der Kunde erhält die Möglichkeit, Einträge in einem Reverse Proxy vorzunehmen.
DDoS-Schutz, Firewall	DDoS-Schutz und Hardware-Firewall können gewählt werden.
vSwitch	Alle Dedicated Server lassen sich mit dem vSwitch in einem vLAN verbinden.
Datenübertragungsrate	Eine Anbindung des Servers von 1 Gbit/s pro Port ist üblich. Einige Provider bieten auch 10 Gbit/s Ports an.
RAID Level	Der Kunde hat die Wahl zwischen RAID 1 (mindestens zwei Festplatten), RAID 5 (mindestens drei Festplatten), RAID 6 (mindestens vier Festplatten) und RAID 10 (mindestens vier Festplatten). Bei den Festplatten hat er die Wahl zwischen SSDs, HDDs und NVMe SSDs in unterschiedlichen Größen. Er hat zudem die Wahl zwischen Hardware-RAID und Software-RAID.
Dedizierte GPU	Als GPU kann z. B. eine Nvidia Tesla oder eine GeForce GT konfiguriert werden.
Images/Software	Beliebte Images, die durch Provider installiert werden können, sind „Debian“, „Fedora“, „Ubuntu“, „CentOS“, „LAMP“ (Linux - Apache - MySQL - PHP), „Proxmox“, „Webmin“, „Windows Server“, „cPanel/ WHM“, „Plesk Obsidian“, „Rescue-System“.
Import eigener Images	Über den Import eigener Images können eigene iso- oder img-Dateien gestartet werden.
Uneingeschränkter Traffic	Der Netzwerk-Traffic wird vonseiten des Providers gerne begrenzt. Ziel sollte ein uneingeschränkter Datenverkehr sein.
Back-up	Back-up-Speicher ist nicht inklusive.
KVM	Über ein KVM (Keyboard Video Mouse) lässt sich auch das BIOS der Hardware aus der Ferne konfigurieren.

LE 2 - Virtual Dedicated Server (VDS)

Bei einem Virtual Dedicated Server mietet der Kunde bei einem Provider/Hoster dedizierte Ressourcen eines Bare Metal. Er mietet also nicht eine komplette Hardware, sondern nur einen Teil davon und teilt sich den Bare Metal mit anderen Kunden. Aus diesem Grund ist die Anzahl der wählbaren Parameter kleiner. Die gebuchten Ressourcen werden exklusiv dem Kunden zugewiesen. Im Gegensatz zu VPS gibt z. B. keine Überprovisionierung.

Folgende Kriterien sind bei der Auswahl zu berücksichtigen:

Technische Anforderungen an Virtual Dedicated Server	
Anzahl Kerne	Der Kunde wählt die Anzahl dedizierter CPU-Kerne. Die Anbieter unterscheiden zwischen physikalischen CPU-Kernen und vCPUs: Verfügt die CPU über Hyper-Threading, so erhält der Kunde bei einem Kern tatsächlich zwei vCPUs. Mietet er eine vCPU dann bleibt es bei diesem einem Rechenkern.
Speicher	Üblich sind bis zu maximal 64 GB Hauptspeicher, weil der gesamte Hauptspeicher mit anderen Kunden geteilt wird.
NVMe-SSD/SSD	Die derzeit „schnellsten“ Festplatten sind sogenannte NVMe-SSDs. HDDs stellen eine Bremse dar und sollten bei Servern vermieden werden. Zusätzlicher Speicherplatz kann als SSD dazu gebucht werden.
Datenübertragungsrate	Bei kleineren VDS wird die nutzbare Bandbreite oft eingeschränkt auf beispielsweise 100 MBit/s.
Uneingeschränkter Traffic	Der Netzwerk-Traffic wird vonseiten des Providers gerne begrenzt. Ziel soll ein uneingeschränkter Datenverkehr sein.
Images/Software	Beliebte Images, die durch den Provider installiert werden können, sind „Debian“, „Fedora“, „Ubuntu“, „CentOS“, „LAMP“ (Linux - Apache - MySQL - PHP), „Proxmox“, „Webmin“, „Windows Server“, „cPanel/WHM“, „Plesk Obsidian“, „Rescue-System“.
Import eigener Images	Über den Import eigener Images können eigene ISO- oder IMG-Dateien gestartet und installiert werden.
Back-up	Back-up-Speicher ist nicht inklusive.

Wichtig: eine hohe Sicherheit erreicht der Kunde durch Verschlüsselung der Laufwerke und Zwei-Faktor-Authentifizierung.

LE 3 - Virtual Private Server (VPS)

Bei einem Virtual Private Server (VPS) mietet der Kunde beim Hoster eine virtuelle Maschine, die er mittels eines webbasierten Control Panels starten, stoppen, installieren, sichern und wiederherstellen kann. Bei VPS teilen sich mehrere Kunden die vorhandenen physikalischen CPU-Kerne.

Folgende Kriterien sind bei der Auswahl zu berücksichtigen:

Technische Anforderungen an Virtual Private Server	
Anzahl vCPU	Anzahl virtualisierter Kerne; bei einem VPS erhält der Kunde die Kerne nicht exklusiv. Die Anzahl CPUs sollte aufgrund des Shared Hosting um mind. 25 % höher gewählt werden, weil die Hardware vom Provider überprovisioniert werden.

Technische Anforderungen an Virtual Private Server	
Speicher	Größe des Hauptspeichers in GB
SSD	Größe des Festplattenplatzes in GB; nach Möglichkeit sind NVMe SSD Speicher aufgrund der höheren Datenraten zu bevorzugen.
Datenübertragungsrate	Netzwerk-Ports sind bei kleineren VPS gedrosselt auf beispielsweise 200 MBit/s.
Uneingeschränkter Traffic	Der Netzwerk-Traffic wird vonseiten des Providers gerne begrenzt. Ziel soll ein uneingeschränkter Datenverkehr sein.
Images/Software	Beliebte Images, die durch den Provider installiert werden können, sind „Debian“, „Fedora“, „Ubuntu“, „CentOS“, „LAMP“ (Linux - Apache - MySQL - PHP), „Proxmox“, „Webmin“, „Windows Server“, „cPanel/WHM“, „Plesk Obsidian“, „Rescue-System“.
Import eigener Images	Über den Import eigener Images können eigene ISO- oder IMG-Dateien gestartet und installiert werden.
Back-up Speicher	Back-up-Speicher wird als ftp-Speicher angeboten. Dieser Speicher wird für die täglichen Sicherungen (Konfigurationsdateien, Datenbankexporte, etc.) der Server benötigt.

LE 4 - Network Attached Storage (NAS)

Bei einem Network Attached Storage (NAS) handelt es sich um einen Dateiserver, welcher im eigenen Netzwerk betrieben wird. Neben den NAS-Systemen für Rechenzentren, diese sind auf höchste Schreib-, Lese- und Übertragungsraten optimiert, gibt es die NAS-Systeme für kleinere und mittlere Netzwerke. Diese sind nicht im 19-Zoll-Format, sondern in einem (Mini-) Towergehäuse untergebracht und bieten zudem einen integrierten Webserver. Darüber lassen sich Serveranwendungen und virtuelle Maschinen auf dem NAS betreiben.

Folgende Kriterien sind bei der Auswahl zu berücksichtigen:

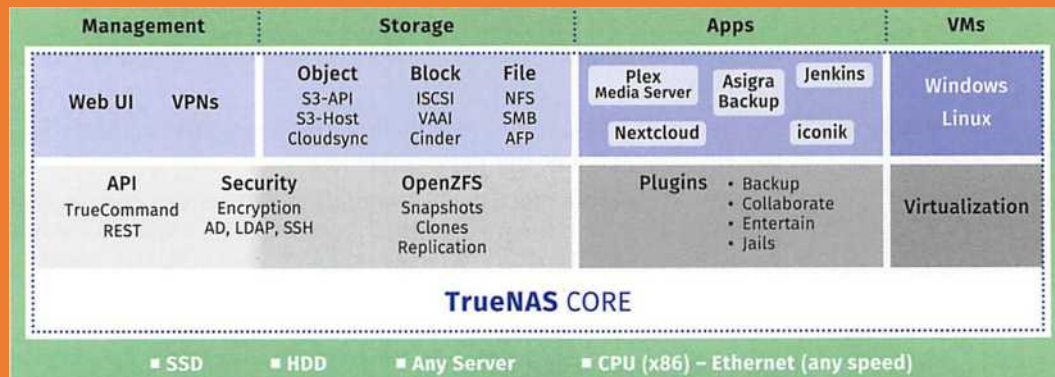
Technische Anforderungen an Network Attached Storage	
Bauform	19-Zoll-Gehäuse für Rack-Montage oder Mini-Tower
Kapazität	maximale Anzahl SSD-Datenträger, maximale Gesamtkapazität
Verschlüsselungsmodul	Unterstützung von Verschlüsselung durch Hardware
Schreib- und Lesegeschwindigkeit	Schreib- und Lesegeschwindigkeit in Megabytes pro Sekunde
RAID Level	Auch bei NAS-Systemen können Festplatten zur Laufzeit ausfallen. Mittels Hardware RAID können einzelne Laufwerke zur Laufzeit gewechselt werden.
Filesystem	Bei Open/FS z.B. handelt es sich um ein Storage-System inkl. Dateisystem, Volume Manager, Snapshots, Copy-on-Write Klones, Remote Replication, Raid-Z u.v.m.
Netzwerkanbindung	Anbindung z. B. über Gigabit-Ethernet; über Link-Aggregation (parallele Nutzung mehrerer Netzwerk-Ports) kann der Datendurchsatz erhöht werden.
Redundantes Netzteil	Mit einem redundanten Netzteil darf auch ein Netzteil ausfallen.

Technische Anforderungen an Network Attached Storage

VM Unterstützung

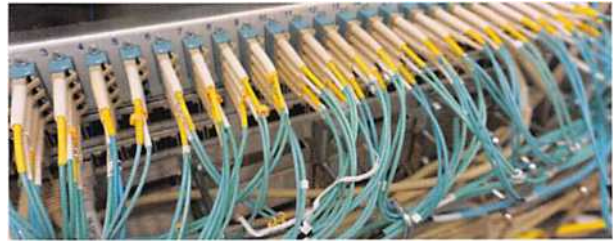
Einige NAS bieten eine Weboberfläche, über welche sich beispielsweise virtuelle Maschinen auf dem NAS einrichten lassen. So lässt sich auf einem NAS zusätzlich z.B. eine VoIP-Telefonanlage betreiben.

Die Open Source "FreeNAS™"/"TrueNAS™ core" ist eine Alternative zu proprietärer NAS-Software. Sie nutzt „Open/FS“ als Filesystem und ist, auf entsprechend performanter Hardware und bei entsprechender Konfiguration, auch für den Gebrauch in Rechenzentren geeignet.



TAG 8 - Technische Anforderungen der Rechenzentren kennen

Für den Aufbau, die Erweiterung und den Betrieb von Rechenzentren werden Komponenten benötigt, die zuverlässig sind und eine sehr hohe Performance liefern. Dabei unterscheiden sich die Anforderungen grundlegend gemäß der Leistungsansprüche des Einsatzbereiches: Sollen High-Performance-Computing oder eine High-Performance-Cloud erstellt werden oder aber Hochsicherheitslösungen, private Rechenzentren, Collocations für Banken und Industrie, Rechenzentren für Internet-Service-Provider oder Telekommunikation?



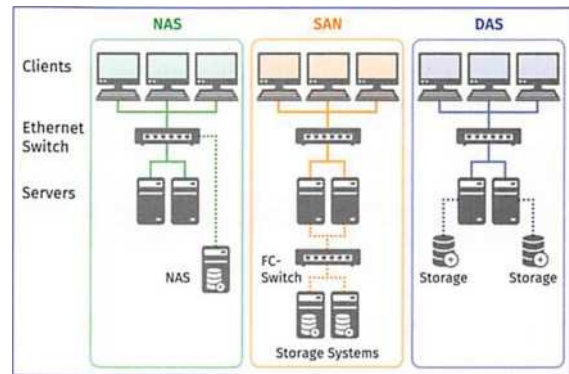
So ist beispielsweise bereits in der Planung für die Verkabelung festzulegen, welche Übertragungsraten erreicht werden müssen, welche Distanzen verlegt werden müssen und welche Dämpfungen einzuhalten sind.

Die folgende Tabelle zeigt die technischen Anforderungen an Rechenzentren:

Technische Anforderungen an Rechenzentren	
LWL-Verkabelung	Verkabelungssysteme mit Lichtwellenleiter benötigen entsprechende Kabel (Singlemode/Multimode), Mehrfaser-Steckverbinder MTP/MPO, Transceiver und aktive Netzwerkkomponenten gemäß den zu unterstützenden Standards, z. B. 400 GBASE-SR8/IEEE 802.3bs 400 G (Terabit Ethernet, TbE)
Kupferverkabelung	Zum Einsatz kommen 10-GBASE-T-SSTP-Kupferkabel, also CAT7- oder CAT6a-Kabel mit entsprechenden Steckern und Netzwerkkomponenten.
KVM-Konsole	Eine 19-Zoll-KVM-(Keyboard Video Mouse)Konsole reicht, um mehrere Server zu bedienen.
Server-Hardware	Die Serverhardware wird von Lieferanten gemäß Geschäftsmodell bezogen. Beidseitig gesicherte Stromkabel verhindern, dass sich Stromkabel lösen.
Server-Software	Um die Rechenleistung an Kunden vermieten zu können, wird eine Software eingerichtet, die es erlaubt, VDS, VPS, Webhosting und Dedicated Server technisch einzurichten, kundenspezifisch bereitzustellen und kaufmännisch abzurechnen.
USV	Ein wichtiges Kriterium ist die Ausgangsleistung der USV. Die Gesamtleistung und Scheinleistung aller Server dürfen die Ausgangsleistung der USV nicht überschreiten. Ein zweites Kriterium ist die Zeit bzw. Dauer, also wie lange die USV den Strom liefern kann. Die USV sollte ebenso bei geringem Akkustand signalisieren können, dass sich die Server herunterfahren müssen. Die Signalisierung erfolgt über RS232, USB oder UTP.
Wärmerückgewinnung	Rechenzentren erzeugen sehr viel Wärme. Um diese Wärme möglichst effizient zu nutzen, kann Flüssigkühlung eingesetzt werden. Dies führt zu hohen Abflusstemperaturen, die dann weiter genutzt werden können. Bei Luftkühlung mit Wärmetauscher und Wärmepumpe sind die Abflusstemperaturen deutlich geringer. Diese Abwärme lässt sich daher kaum im Nahwärmenetz nutzen.

LE 1 - NAS - SAN - DAS

Bei NAS, SAN und DAS handelt es sich um Storage für höchste Datendurchsätze und große Datenmengen, sprich: für Server in Rechenzentren. Da Storage so performant wie möglich arbeiten sollen, werden in Rechenzentren bisher separate Netzwerke, sogenannte Storage Area Networks, eingerichtet mit 10 Gbit/s Datenübertragungsrate und mehr.



NAS, SAN, DAS im Vergleich		
Network Attached Storage (NAS)	Storage Area Network (SAN)	Direct Attached Storage (DAS)
Storage, welches via Ethernet in einem Netzwerk bereitgestellt wird.	Ein SAN ist über Fibre Channel mit allen Servern verbunden.	Der Storage wird direkt an einen Server angeschlossen, z. B. über Serial Attached SCSI (SAS).
Clients befinden sich im gleichen Netz wie das NAS.	Die Clients greifen über Ethernet auf die Server zu.	Anschluss einer einzelnen Festplatte oder eines JBODs (Just a bunch of Disks) ist möglich.
Einer einfachen Anbindung steht die Belastung des LANs gegenüber.	Hochpreisig, erlaubt aber hohe Transferraten für alle Server.	Ist kostengünstig, aber exklusiv an einem Host verfügbar.

LE 2 - Unterbrechungsfreie Stromversorgung (USV)

Eine unterbrechungsfreie Stromversorgung (Uninterruptable Power Supply, UPS), versorgt elektrische Geräte mit Strom, wenn die Hauptstromversorgung ausfällt.



USV-Klassifizierung nach DIN EN 62040-3/IEC 62040-3 - Stufe I	
VFI	USV der Klasse VFI arbeiten <u>spannungs- und frequenzunabhängig</u> (Voltage and Frequency independent, VFI). Sie schützen gegen alle Arten von Spannungsschwankungen, -stößen, Unter- und Überspannung, Blitzeinwirkungen, Schaltspitzen, Stromausfällen und Frequenzänderungen. Sie eignen sich daher für alle Einsatzszenarien wie Rechenzentren, Server und Netzwerke.
VI	USV der Klasse VI arbeiten <u>spannungsunabhängig</u> vom Netz (Voltage Independent). Sie schützen vor Spannungsproblemen und Stromausfällen. Sie sind günstiger als VFI und sind für kleinere Netzwerke geeignet.
VFD	USV der Klasse VFD arbeiten <u>spannungs- und frequenzabhängig</u> vom Netz (Voltage and Frequency dependent, VFD). Sie sind günstiger als VI Systeme und sind geeignet für den Schutz einzelner Arbeitsplätze.

USV bestehen aus Akkus, die sich entladen, sobald die Hauptstromversorgung ausfällt. Sie haben daher eine begrenzte Kapazität.

Bei der Auswahl von USV muss die Gesamtlast berücksichtigt werden, die alle zu schützenden Geräte aufnehmen, und ebenso die Betriebszeit. Diese gibt die Dauer in Minuten an, in der die USV Strom liefern soll. Bei einem einzelnen Server sind dies beispielsweise 20 Minuten.

Über eine Schnittstelle, z. B. RS232, USB oder RJ45, teilt sie den zu schützenden Komponenten mit, wann diese herunterfahren müssen.

LE 3 - WAN-Infrastrukturen unterscheiden

Telekommunikations-, Kabelnetz- und Mobilfunknetzbetreiber stellen den Betrieb der WAN-Netze (Wide Area Network) sicher. Da es bei der Anbindung von Netzwerken i.d.R. immer um Datenübertragungsraten geht, gibt die folgende Tabelle eine Übersicht darüber:

Datenübertragungsraten von WAN-Netzen	
Glasfaser	Bei Glasfaser sind Datenübertragungsraten bis 10 Gbit/s möglich (Stand: 2021).
Kabelfernsehtnetz	Beim Kabelfernsehtnetz werden Datenraten von 10 Gbit/s im Downstream und 1 Gbit/s im Upstream erreicht.
Mobilfunknetz	Bei 5G, dem Mobilfunknetz der fünften Generation, sind Datenraten von bis zu 10 Gbit/s möglich.
Kupferkabel/ DSL	Bei VDSL2 sind bei sehr kurzen Kabelstrecken theoretische Datenraten von bis zu 350 Mbit/s in der Summe (Upstream und Downstream) möglich. Bis zu einer Entfernung von 500 Metern sind Datenraten in der Summe von bis zu 100 Mbit/s möglich. Bei Entfernungen über 500 Meter sinkt die Rate auf 50 Mbit/s. Je größer die Entfernung ist, desto größer ist die Dämpfung.

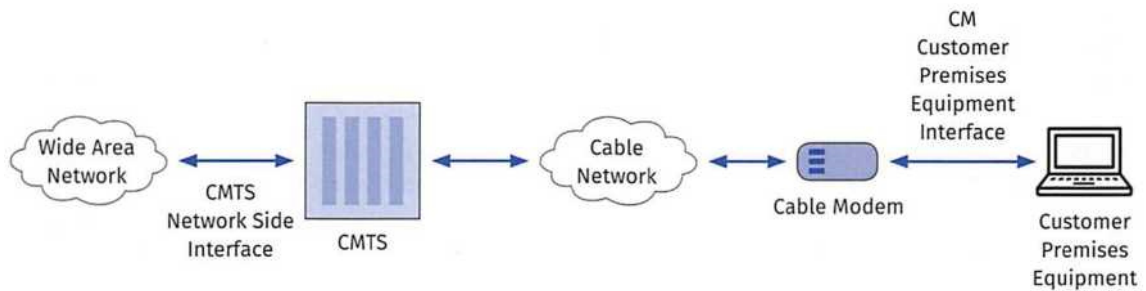
(1) Glasfasernetz

Die Telekommunikationsbetreiber verlegen in vielen Gebieten Deutschlands Glasfaserkabel (Fiber to the home, FTTH). Dabei wird „der letzte Meter“ vom Verteilerkasten (siehe nebenstehende Abbildung) mittels eines Glasfaserleerrohrs zum sogenannten Hausübergabepunkt geführt. Die Glasfasern selbst werden mit Druckluft durch die Leerrohre zum Hausübergabepunkt „geschossen“. An diesem werden die Glasfasern einzeln herausgeführt und mit Glasfasersteckern versehen. Ein biegeunempfindliches Glasfaserinnenkabel wird zum optischen Netzwan- dler (Optical Network Termination, ONT) verlegt. Dieser wandelt das Laserlicht in ein elektrisches Signal um. Ab hier übernimmt der Kunde den Anschluss seines Netzwerks.



(2) Kabelfernsehnnetz

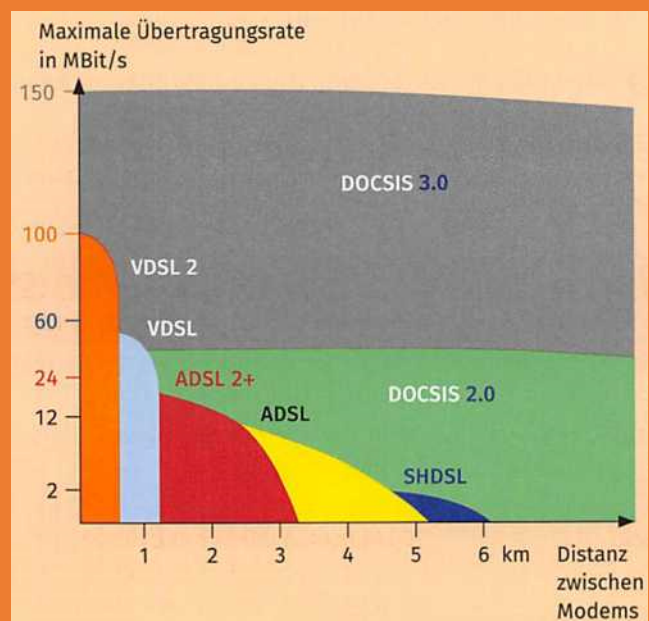
Das Kabelfernsehnnetz besteht aus dem Cable Modem Termination System (CMTS) dem Cable Network (Koaxialkabeln) und den Endgeräten (Cable Modem). Das folgende Schaubild zeigt die Zusammenhänge gemäß der Spezifikation DOCSIS-3.1.



Beim Kabelfernsehnnetz werden die Daten mittels sogenannter Kabelmodems auf Trägersignale moduliert, ähnlich DSL. Die Data over Cable Service Interface Specification (DOCSIS) erlaubt den Transport von IP-Paketen in beide Richtungen. Dabei werden im Kabelfernsehnnetz deutlich höhere Übertragungsraten erreicht als bei DSL (siehe Abbildung): Gegenüber der DSL-Technik sind auch die Übertragungstrecken deutlich größer.

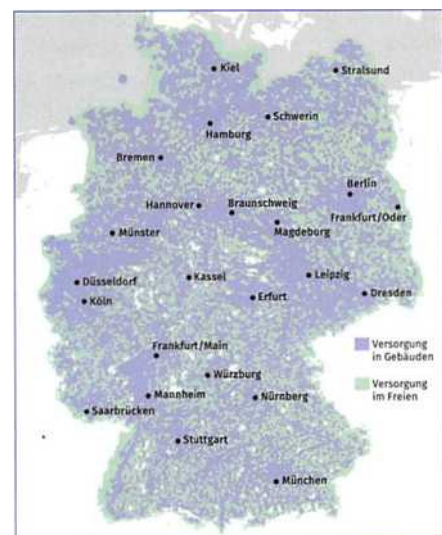
Mit Abschaltung der analogen Technologie werden zusätzlich zu DOCSIS 3.0 die freien Frequenzen mit Übertragungskkanälen der aktuellen

DOC- SIS-3.1-Spezifikation belegt Hierbei sind technisch maximal Download- Raten von bis zu 1 Gbit/s und Upload-Raten von bis zu 240 MBit/s möglich. Mit DOCSIS 4.0 werden die Datenübertragungsraten noch einmal erhöht. Die DOCSIS-Spezifikation für Europa basiert auf dem PAL-Fernsehsystem und nennt sich EuroDOCSIS.



(3) Mobilfunknetze

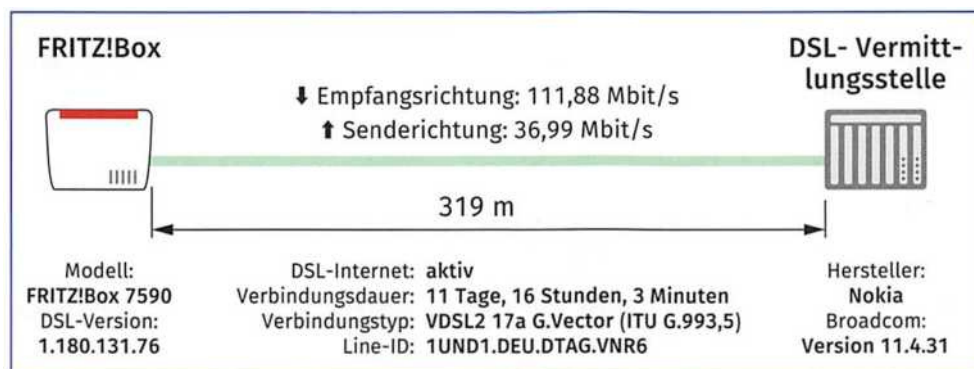
Die Mobilfunknetzbetreiber von D1, D2, O2 und E-Plus stellen die GSM-, GPRS-, UMTS- und LTE-Netze bereit. Über sogenannte Verfügbarkeitskarten lässt sich online einsehen, ob das entsprechende Mobilfunknetz am gewünschten Standort zur Verfügung steht (siehe Abbildung).



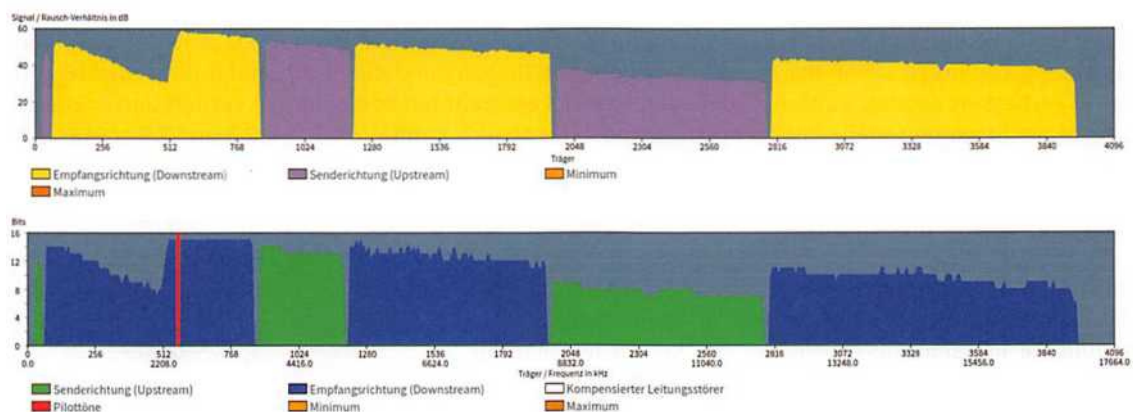
Mobilfunknetze	
GSM	Global System for mobile Communications (GSM) bezeichnet ein Mobilfunknetz der zweiten Generation. Es ermöglicht Datenübertragungsraten von bis zu 9,6 Kbit/s.
GPRS	Bei General Packet Radio Service (GPRS) handelt es sich ebenfalls um ein Mobilfunknetz der zweiten Generation. Es ermöglicht Datenübertragungsraten von bis zu 55 Kbit/s.
UMTS	Bei Universal Mobile Telecommunications System (UMTS) handelt es sich um ein Mobilfunknetz der dritten Generation. Es ermöglicht Datenübertragungsraten von bis zu 384 Kbit/s. High Speed Packet Access (HSPA) ist eine Erweiterung und ermöglicht Datenübertragungsraten von bis zu 7,2 MBit/s. Das UMTS Netz/3G wurde in Deutschland 2021 abgeschaltet.
LTE	Long Term Evolution (LTE) ist das 4G-Netz. Hierüber sind Datenraten von bis zu 100 MBit/s möglich, mit LTE Advanced von bis zu 1 Gbit/s.
5G	5G ist eine Erweiterung zu LTE und ermöglicht Datenraten von bis zu 10 Gbit/s.

(4) Kupferkabel/DSL

Die Telekommunikationsbetreiber stellen Netzwerke auf Basis einfacher Kupferkabel zur Verfügung, die Teilnehmeranschlussleitungen (Digital Subscriber Line, DSL). Mittels der DSL-Technik kommunizieren DSL-Modems/-Router mit DSL-Access-Multiplexern (DSLAM). Dabei wird das Netzwerkprotokoll „PPP over Ethernet“ verwendet. Die DSLAM sind über Gigabit-Ethernet mit dem Glasfaser-Backbone verbunden. Das folgende Schaubild zeigt die DSL-Informationen einer Fritz!Box, die mit einer DSL-Vermittlungsstelle in 319 Metern Entfernung verbunden ist.



Die folgende Grafik zeigt die Frequenzbereiche, die bei dem obigen Kunden auf dem Kupferkabel genutzt werden. Aufgrund der geringen Entfernung von nur 319 Metern ist das Signal/Rausch-Verhältnis für alle Frequenzen groß genug.



Kupferkabel	
CAT5-Kabel	Kupferkabel der Spezifikation CAT5 werden heute (Stand: 2021) für die strukturierte Verkabelung von Netzwerken genutzt. Sie eignen sich für Übertragungsraten von bis zu 1 Gbit/s bzw. 1000 Base-T (Gigabit Ethernet). Sie sind mit RJ45-Steckern erhältlich und ebenso als Meterware.
CAT6a-Kabel	Kupferkabel der Spezifikation CAT6 eignen sich für Übertragungsraten von bis zu 10 Gbit/s (10 GBASE-T). Die maximale Länge des Kabels darf 100 Meter nicht überschreiten. Als Stecker kommen auch hier RJ45 zum Einsatz.
CAT7-Kabel	CAT7-Kabel sind gemäß IEEE802.3an für 10 GBASE-T geeignet. Aufgrund der hohen Frequenzen können keine RJ45-Stecker genutzt werden. Bei den Kabeln handelt es sich um Screened-Shielded-Twisted-Pair-/S/FTP-Kabel: Jedes der vier Adernpaare ist geschirmt mit einem Drahtgeflecht. Es gibt zusätzlich ein Drahtgeflecht um alle vier Adernpaare insgesamt.

TAG 9 - Wirtschaftliche und sicherheitsrelevante Anforderungen sowie Nachhaltigkeit in Netzwerken berücksichtigen

LE 1 - Wirtschaftliche Anforderungen berücksichtigen

Wirtschaftliche Entscheidungen und Anforderungen sind für viele Gremien und Stakeholder von hoher Bedeutung. Mit ihnen sollen der ressourcenschonende Umgang und die Profitabilität des Projektergebnisses verbessert werden. Zunächst sollten alle bereits erarbeiteten Kompetenzen vertieft und in Erinnerung gebracht werden.

LE 2 - Make- or Buy-Entscheidung

Eine Make-or Buy-Entscheidung ist eine Entscheidung über die Eigenfertigung oder den Fremdbezug eines Produkts. Viele Argumente müssen abgewogen werden, um diese Entscheidung schlüssig treffen und begründen zu können.

Aufgrund des Fachkräftemangels und der vielen technologischen Entwicklungen sind Unternehmen bei der Beschaffung und Bereitstellung von Netzwerken auf fremde Unterstützung angewiesen. Sie prüfen sogar das Outsourcing ganzer IT-Bereiche und -Dienste.



Make-or-Buy-Entscheidung	
Argumente für „Make“ und gegen „Buy“	Argumente für „Buy“ und gegen „Make“
• freie Personalkapazitäten der Fachleute vorhanden • Kernkompetenz und Technologieführerschaft, Lerneffekte • Geheimhaltung von Know-how, Wettbewerbsvorteile • guter Marktzugang im Unternehmen vorhanden	• keine freien Mitarbeiterkapazitäten • eigene Machbarkeit nicht gegeben • Vorhaben nicht im Kernkompetenzbereich • Inhouse-Kompetenzen nicht ausreichend • Marktzugang für Eigenbeschaffung nicht gut • hohe Innovationsziele bedürfen externe Expertise
Entscheidend für „Make or Buy“	
• strategische Ausrichtung bzw. Unterstützung der Stakeholder für eine Variante • Zeitvergleiche (Herstellungsdauer, Umstellungszeit) und Notwendigkeit einer pünktlichen Erstellung • Kostenvergleich und Wirtschaftlichkeit (Kosteneinsparungen) • Liquidität für das Vorhaben • Fachkompetenzen für Vorhaben vorhanden oder dadurch erweiterbar • Risikobetrachtungen, z.B. Kosten, Zeit, Qualität/Erfolg, Betriebsausfall, Lieferantenrisiken	
Alternativen: Outsourcing, Teiloutsourcing, Eigenleistung einbringen	

LE 3 - Anschaffungs- und Betriebskosten

Viele Beschaffungsprojekte scheitern, weil die Anforderungen nicht genau genug spezifiziert wurden und darauf aufbauend Kosten falsch oder unzureichend bemessen wurden. Evtl. verzichtet man auch weitgehend auf wirtschaftliche Betrachtungen. In der Folge kommt es häufig zu Kürzungen und Änderungen, die zu großer Unzufriedenheit im Team führen. Ergänzend zu den bisherigen Modulen sollen daher die folgenden Aspekte herausgestellt werden.

Nach dem HGB gehören zu den Anschaffungskosten alle Kosten, die bis zur völligen Bereitstellung der Netzwerke entstehen. Die Projektleitung hat ständig Kostenübersichten zu erstellen und Kostenkontrollen durchzuführen, Genehmigungsgremien haben Rechenschaft abzulegen.

Anschaffungskosten und Betriebskosten

Anschaffungskosten bei Beschaffung für eigene Zwecke (interne Kunden)

Anschaffungskosten sind nach § 255 HGB alle Aufwendungen, die geleistet werden, um einen Vermögensgegenstand zu erwerben und ihn in einen betriebsbereiten Zustand zu versetzen. Dazu gehören also auch Nebenkosten wie Beschaffungskosten, Installations- und Einweisungsaufwendungen, abzüglich aller Nachlässe, z. B. Rabatte, Skonto.

Betriebliche Kosten bei Lieferung an externe Kunden im Handelsbereich

- Handlungskosten: alle Kosten (betriebliche Aufwendungen), die aufgrund von Handelsleistungen (Umsatzerlöse aus Handelsgeschäften) entstanden sind (Wareneinsatz nicht mitgerechnet) und in die Preise einkalkuliert werden sollen
- Wareneinsatz: Kosten für die beschafften Teile inklusive Bezugskosten, z. B. Transportkosten

Diese Kosten werden in der Handelskalkulation berücksichtigt.

Betriebliche Kosten im Fertigungsbereich (Produktion)

Materialkosten = Materialkosteneinsatz + Materialgemeinkosten

Fertigungskosten = Fertigungslöhne + Fertigungsgemeinkosten

Herstellkosten = Materialkosten + Fertigungskosten

Selbstkosten = Herstellkosten + Verwaltungs- und Vertriebsgemeinkosten

Gemeinkosten sind einem Produkt oder Auftrag nicht direkt zurechenbare Kosten des Betriebs, sie werden über einen Zuschlagsatz pauschal aufgeschlagen.

Betriebliche Kosten im Dienstleistungsbereich

z.B.

projektbezogene Einzelkosten nach Belegen: siehe z. B. Buchung auf Kostenstelle des Projekts

+ projektbezogene kalkulatorische Einzelkosten: z. B. für Arbeitslöhne, direkt zurechenbare Kosten

+ Aufschlag für Gemeinkosten (nicht direkt zurechenbare Kosten: z. B. allgemeine Verwaltung)

= Projektkosten

Cloud-Preis- oder Kostenmodelle für die Bereitstellung (Provisionierung) von Cloud-Diensten, z.B. Pay-per-Use, Pay-as-you-Go (On-demand-Preismodell, nutzungsbasierte Bezahlung)

Man muss flexibel nur die IT-Ressourcen bezahlen, die auch tatsächlich genutzt werden. Eine Anmeldung ist bei dieser Option in der Regel kostenlos und unkompliziert, die Bereitstellung von Cloud-Diensten innerhalb weniger Minuten erfolgt. Am Ende der Abrechnungsperiode, z. B. Monat, erhält man eine detaillierte Auflistung der zeitlichen Nutzung sämtlicher in Anspruch genommenen Services.

Einsatzbereiche: Unternehmen mit großen saisonalen Schwankungen, Unternehmen, die ihren Bedarf nicht einschätzen können, Start-ups, da Einstieg/Test kostengünstig.

- **Reserved** (reserviert fixe Abnahmeleistung): Hier reserviert man sich per Vertrag festgelegte Leistungen (z.B. 10 virtuelle CPUs, 2 TB Speicher und 20 GB Arbeitsspeicher) für eine festgelegte Zeit und erhält dadurch eventuell hohe Rabatte wegen der gesicherten Abnahme, muss allerdings auch zahlen, wenn man die vereinbarte Leistung nicht abnimmt.
- **Combined** (halb „pay-per-use“, halb "reserved"): Eine Kombination von verbrauchsabhängigen und vertraglich fixierten Kosten bietet sich an, wenn man mit Rabatten eine Grundlast vereinbart und bei Mehrbedarf "on demand" Mehrleistungen nach einem vereinbarten Preismodell hinzubuchen kann. Dies ist auch bei Leistungsschwankungen eine gute Alternative.
- **Pay as you grow** (mehrstufiges Kostenmodell mit kostenloser Startphase): Für Start-ups und Innovationsprojekte kann es sinnvoll sein, mit dem Cloud-Provider eine kostenlose Startphase, dann eine kostengünstige Anlaufphase und eine Normalkostenphase zu vereinbaren.

LE 4 - Kalkulation, Angebotsvergleiche und Finanzierung

Für Auftragnehmer und Auftraggeber ist es wichtig, Kostenkalkulationen vornehmen zu können und damit die wirtschaftliche Umsetzung des Projekts einschätzen zu können. Ergänzend sollten Nutzwertanalysen erstellt und Möglichkeiten einer Finanzierung aufgezeigt werden können.

Preisbildung, Beschaffungs- und Angebotskalkulationen

Preise

Preise bilden sich im Markt durch individuelle Entscheidungen von Verkäufern, zu diesem Preis zu verkaufen, und Käufern, zu diesem Preis zu kaufen, entsprechend Angebot und Nachfrage.

Kalkulationsvorlagen

Kalkulationsvorlagen dienen als Hilfsmittel zur Selbstkosten- und Preisbestimmung sowie zu Angebotsvergleichen.

Preiskalkulation - Ein- und Verkauf von Handelserzeugnissen

Werden Handelswaren eingekauft, berücksichtigt die Handelskalkulation für die Ermittlung der Selbstkosten gewährte Rabatte und Skonto der Lieferanten, berechnete Bezugskosten (z. B. für Transport und Versand) und i.d.R. einen Aufschlag für ihre Handlungskosten zur Abdeckung der sonstigen betriebsnotwendigen Kosten für Einkauf und Verkauf. Bei Beschaffungen für eigene Zwecke muss für die Selbstkostenermittlung ein geringerer Aufschlag angesetzt werden. Werden die bezogenen Erzeugnisse an externe Kunden weiterverkauft (Handelsware), werden je nach Marktsituation ein angemessener Gewinnzuschlag und je nach Standardangebot an Nachlässen Zuschläge vorher hinzukalkuliert.

Listeneinkaufspreis	Einkauf
- Liefererrabatt	
= Zieleinkaufspreis	
Liefererskonto	
= Bareinkaufspreis	
+ Bezugskosten	
= Bezugspreis	
+ Handlungskosten (Ein-/Verkauf)	
= Selbstkosten	
+ Gewinnzuschlag	Verkauf
= Barverkaufspreis	
+ Kundenskonto	
= Zielverkaufspreis	
+ Kundenrabatt	
= Listenverkaufspreis netto	
+ Umsatzsteuer	
= Listen-VK inkl. MwSt.	

Stundensatzberechnung

Der Stundensatz von Mitarbeitern in der Rechnungserstellung an Kunden hängt davon ab, wie viele Stunden des Arbeitseinsatzes in Rechnung gestellt werden (verrechenbare Arbeitsstunden) und welche sonstigen nicht verrechneten Mitarbeiterstunden und sonstige Gemeinkosten darüber pauschal bzw. mit einem Prozentaufschlag abgerechnet werden sollen.

Bruttolohn = Nettolohn (Auszahlungsbetrag) + Arbeitnehmerbeiträge Sozialversicherung (Kranken-, Renten-, Arbeitslosen-, Pflegeversicherung) + Steuerabzug (Lohn- und evtl. Kirchensteuer)

Auszubildende erhalten eine **Ausbildungsvergütung**.

Arbeitgeberanteil: Arbeitgeberbeiträge zu den Sozialabgaben (Kranken-, Renten-, Arbeitslosen-, Pflegeversicherung), die betriebliche Unfallversicherung trägt der Arbeitgeber voll

Selbstkosten = Bruttolohnkosten + Arbeitgeberanteil + pauschaler Gemeinkostenaufschlag

Selbstkostensatz = Selbstkosten / produktive (verrechenbare) Arbeitsstunden

Netto-Stundensatz = Selbstkostensatz + Gewinnaufschlag

Selbstkostenkalkulation in der Eigenfertigung (Make-Entscheidung)

Selbstkosten bzw. Bezugskosten von Komponenten, Material, Kleinteilen
+ Selbstkosten Arbeitseinsatz (Stunden · Stundenselbstkostensatz)
+ Zusatzkosten (z.B. Kosten der Beratung und Unterstützung nach Rechnungen der Kostenstelle)
= **Gesamtselbstkosten**

oder

Fixe Kosten (Feste Kosten unabhängig von der Leistungserbringung, z.B. der Kostenstelle)
+ Variable Kosten Arbeitseinsatz (Stunden · Stundenselbstkostensatz)
+ Sonstige variable Kosten (z. B. Energie-, Kommunikations-, Lizenz-, Servicekosten)
= **Gesamtselbstkosten**

Öffentliche Auftraggeber (z.B. Bund, Länder und Gemeinden) dürfen Aufträge für Lieferungen und Leistungen grundsätzlich nur im Wege eines nach VOB geregelten Vergabeverfahrens ausschreiben. Nach der Eignungsprüfung der Anbieter erfolgen eine inhaltliche Wertung der eingegangenen Angebote und die Ermittlung des wirtschaftlichsten Angebots. Angebote werden über Vergabeportale veröffentlicht und lassen sich auch per „eVergabe“ bearbeiten (siehe z.B. www.deutsches-ausschreibungsblatt.de). Die Projektleitung kann über Nutzwertanalysen tabellarisch Vergleiche anstellen.

Angebotsvergleiche durch Nutzwertanalyse

Quantitativer und qualitativer Angebotsvergleich Angebote können mithilfe der Tabellenkalkulation und Kalkulationsblättern vergleichbar gemacht werden, um damit das wirtschaftlichste Angebot zu ermitteln. Dabei kommen nur die Angebote in die engere Wahl, die die Leistungskriterien des Pflichtenheftes erfüllen sowie die pünktliche und ordnungsgemäße Auftragserfüllung garantieren können. Über die Nutzwertanalyse können auch sonstige Zuschlagskriterien (qualitative Entscheidungskriterien) gewichtet einbezogen werden.

	A	B	C	D	E	F
1	Quantitativer und Qualitativer Angebotsvergleich					
2		ACI		JKU		
3	Kalkulation	Eingabe	Ausgabe	Eingabe	Ausgabe	
4	Listeneinkaufspreis	5.000,00 €	5.000,00 €	6.000,00 €	6.000,00 €	
5	- Liefererrabatt	7%	350,00 €	10%	600,00 €	
6	= Zieleinkaufspreis		4.650,00 €		5.400,00 €	
7	- Liefererskonto	3%	139,50 €	2%	108,00 €	
8	= Bareinkaufspreis		4.510,50 €		5.292,00 €	
9	+ Bezugskosten	100,00 €	100,00 €	140,00 €	140,00 €	
10	= Bezugspreis (Einstandspreis)		4.610,50 €		5.432,00 €	
11	Bewertung: quantitativer/qualitativer Vergleich					
12	Entscheidungskriterien	Gewichtung in %	Punkte	Gewichtete Punkte	Punkte	Gewichtete Punkte
13	Preis	40	4	160	3	120
14	Produktqualität	10	4	40	5	50
15	Kompetenz	10	4	40	5	50
16	Verhalten bei Reklamation	15	4	60	5	75
17	Service u. Support	10	4	40	5	50
18	Bisherige Zusammenarbeit	15	4	60	5	75
19	Summe	100		400		420
20	Hinweis:	Punktvergabe: 1 = schlecht bis sehr gut=5				

Wirtschaftlichstes Angebot

Am wirtschaftlichsten ist das Angebot mit dem besten Preis-/ Leistungsverhältnis. Dieses wiederum wird anhand von Zuschlagskriterien wie etwa Qualität, Preis, Umwelteigenschaften, Zweckmäßigkeit, Betriebskosten, Lebenszykluskosten etc. gewichtet und bewertet. Im öffentlichen Bereich (Kommunen, Behörden, staatliche Einrichtungen) müssen Vergabeverordnungen (VOB) und -richtlinien eingehalten werden. Leistungs- und Zuschlagskriterien müssen bereits in der Auftragsbekanntmachung öffentlich gemacht werden.

Bei der Feststellung der wirtschaftlich besten Lösung werden auch Amortisationsrechnungen und TCO- Analysen durchgeführt.

Wirtschaftlichkeitsanalyse

Wirtschaftlichkeit

Wirtschaftlichkeit ist allgemein gegeben, wenn die aus der Beschaffung entstehenden Erlöse höher sind als die Erträge, somit eine Wirtschaftlichkeit = Erlöse/Kosten > 1.

ROI und Amortisationsrechnung

ROI bedeutet Return on Investment (Anlagenrendite) und gibt als Kennzahl das Verhältnis von Investitionskosten zu Investitionsrückflüssen an. Dieses sollte mindestens 1 sein, damit die Investition keinen materiellen Verlust gebracht hat (in % mindestens 100 %).

Aus der Gesamtnutzungszeit und dem ROI-Wert kann die Amortisationszeit (frz. *amortir*: tilgen = Tilgungszeit), also die Zeitdauer, berechnet werden, in der die Kosten der Investitionen durch die Rückflüsse (Erträge) gedeckt wurden.

Beispiel: Investitionssumme = 60000,00 €, kalkulierte Rückflüsse 3 Jahre monatlich 2

500,00 € ROI = Rückflüsse / Investitionskosten = 90000 / 60000 = 1,5

Amortisation(zeit) = Nutzungsdauer / ROI oder Nutzungsdauer • Investitionskosten / Rückflüsse = 36/1,5

= 24 Monate oder 36 • 60 000 / 90000 = 24 Monate

TCO-Betrachtung

Beim TCO werden in die Investitionsentscheidung nicht nur die Anschaffungskosten einbezogen, sondern möglichst alle weiteren direkten und indirekten Kosten (Total Costs), z. B. Energie-, Reparatur- und Wartungskosten, Organisations- und sonstige Schulungskosten, zusätzlicher Verwaltungsaufwand, Entschädigung für entgangene Geschäfte etc. Diese Definition ist beim Angebotsvergleich zu berücksichtigen. Sehr schwierig ist häufig die exakte Kostenermittlung. Es gibt unterschiedliche Ansätze, den TCO zu berechnen, z. B. des VDI.

Nicht immer ist die Finanzierung von Projekten einfach. Die Projektleitung wird bei Finanzierungsvergleichen einbezogen und aufgefordert, diese zu erstellen oder daran mitzuwirken.

Finanzierung und Leasing von Vorhaben sowie Miete von Cloud-Diensten

Entscheidung zwischen Kauf mit Finanzierung und Leasing

Beim Kauf geht das Gut in das Eigentum über, beim Leasing nur in den Besitz. Der Eigentümer hat mehr Rechte und ist nicht von den Vertragsbedingungen des Leasinggebers abhängig, bei Leasing ist aber ein laufender Wechsel auf Neugeräte möglich; ein Kostenvergleich mit einer Finanzierungsoption ist sinnvoll.

Finanzierung über ein Darlehen

- Fälligkeits- bzw. Festdarlehen bzw. endfälliges Darlehen
- Ratendarlehen- bzw. Tilgungs- bzw. Abzahlungsdarlehen
- Annuitätendarlehen: Darlehen mit festen Kreditraten und gleichem Zinssatz, aufgrund der Tilgung immer größerer Tilgungsanteile

Leasing

Gebrauchsüberlassung eines Gebrauchsgutes auf Zeit, gegen Entgelt im Rahmen eines „besonderen Vertrages“. Im Gegensatz zur Miete übernimmt der Leasingnehmer i.d.R. alle üblichen Eigentümerpflichten wie Unterhalt, Wartung und Instandhaltung, Risiken des Verlustes u.Ä. Die Finanzierung über Leasing übernehmen grundsätzlich Leasinggesellschaften, sodass der Auftragnehmer den Rechnungspreis vom Leasinggeber bezahlt bekommt.

Miete oder Cloud-Services

IaaS, PaaS, FaaS, SaaS

Zur Präsentation von Zwischenberichten (z.B. auf Milestone-Sitzungen) und zum Projektabschluss muss die Projektleitung Soll-Ist-Vergleiche anstellen und ihre Controlling-Anstrengungen nachweisen.

Projektcontrolling zum Projektabschluss

Zwischen- und Nachkalkulationen

Die Projektleitung ist angehalten, während und zum Abschluss des Projekts Kostenübersichten zu erstellen.

Überschussrechnung bei Kundenprojekt: Gewinn = Erlöse - Kosten

Wirtschaftlichkeit = Erlöse/Kosten > 1

Soll-Ist-Vergleiche

Zeitlich: Es werden Übersichten geführt, ob die zeitlich vorgenommenen Kalkulationen eingehalten wurden oder ob es Abweichungen gegeben hat.

Kosten, ggf. Erlöse: Es werden von der Projektleitung laufend bzw. abschnittsweise (Milestones) Kostenvergleiche durchgeführt und Abweichungen ermittelt.

TAG 10 und TAG 11 - Sicherheitsrelevante Anforderungen berücksichtigen

In diesem Kapitel werden die Kompetenzen zu IT-Sicherheitsgrundlagen und der Schutzbedarfsanalyse im Rahmen der Bereitstellung von Netzwerken vertieft und erweitert. Je nach Ausbildungsberuf der IT-Berufe erfolgt eine weitere Kompetenzerweiterung in späteren Modulen.

LE 1 - Schutzbedarf für Netze analysieren

Jeden Tag werden tausende von Malware-Bedrohungen an Unternehmen und Organisationen gerichtet, die abgewehrt werden müssen. Werden Bedrohungen nicht abgewehrt, können Unternehmen so stark geschädigt werden, dass Betriebsstillstand und letztendlich sogar die Insolvenz bzw. Unternehmensaufgabe drohen können.

Es gibt eine Vielzahl verschiedener Angriffsformen und Schwachstellen, um über diese die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu stören. Unter dem Oberbegriff „Verhinderung von Diensten“ (Denial of Service) oder auch DoS-Angriff können von intern oder extern Angriffe erfolgen, indem ein Angreifer diese Ressourcen (Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität) so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen.



Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat über die Einrichtung und Pflege des Grundschutzkompendiums ein Basiswerk geschaffen, um die Unternehmen bei der Einrichtung eines ISMS zu unterstützen. Das BSI weist auf folgende Gefährdungslagen in der Netzbereitstellung hin:

BSI – Gefährdungsbeurteilung zur Netzbereitstellung (Auswahl)

Gefährdungsbeurteilung für Netzarchitektur und -design (NET.1.1)

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.27 Ressourcenmangel
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten, Systemen
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.43 Einspielen von Nachrichten
- G 0.46 Integritätsverlust schützenswerter Informationen

Ergänzende Gefährdungsbeurteilung für Netzmanagement (NET.1.2)

- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen

Ergänzende Gefährdungsbeurteilung für WLAN-Betrieb (NET.2.1)

- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Ergänzende Gefährdungsbeurteilung für Router und Switches (NET.3.1)

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten, Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust

Ergänzende Gefährdungsbeurteilung für Firewall (NET.3.2)

- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.39 Schadprogramme
- G 0.41 Sabotage

Ergänzend bedeutet: vorgenannte Gefährdungen können auch eintreten!

Mängel in der Informationssicherheit führen zu:
Verlust der Verfügbarkeit, der Vertraulichkeit der Informationen und der Integrität (Korrektheit) von Informationen

In der Gefährdungsbeurteilung des BSI wird angegeben, welche Grundwerte der Informationssicherheit (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) durch die notwendigen Anforderungen vorrangig geschützt werden. Dazu werden grundsätzliche Einschätzungen zur Eintrittshäufigkeit, zu den Auswirkungen und zum Risiko gegeben, um eine Risikoanalyse zu erleichtern.

Risikoanalyse und -behandlung

Gefährdungsbeurteilung für Server (Beispiel, Auszug)

Basiseinstellung zur Beurteilung entsprechend BSI zur Diskussion mit dem Kunden

Gefährdung (bedrohte Grundwerte)	Eintrittshäufigkeit	Auswirkungen	Risiko
G 0.8 Ausfall oder Störung der Stromversorgung (A)	selten	begrenzt	mittel
G 0.9 Ausfall oder Störung von Kommunikationsnetzen (A)	häufig	begrenzt	mittel
G 0.14 Ausspähen von Informationen (Spionage) (C)	mittel	begrenzt	gering
G 0.23 Unbefugtes Eindringen in IT-Systeme (C, I, A)	mittel	beträchtlich	mittel
G 0.25 Ausfall von Geräten oder Systemen (A)	mittel	beträchtlich	mittel
G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen	selten	beträchtlich	mittel
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	beträchtlich	mittel
G 0.32 Missbrauch von Berechtigungen (C, I, A)	selten	beträchtlich	mittel

Auswirkungen/Schadenshöhe

↑

existenzbedrohend

beeinträchtlich

begrenzt

vernachlässigbar

↓

mittel	hoch	sehr hoch	sehr hoch
mittel	mittel	hoch	sehr hoch
gering	gering	mittel	hoch
gering	gering	gering	gering
selten	mittel	häufig	sehr häufig

Eintrittshäufigkeit →

Risikobehandlung

Umsetzungsplanung:

- Zielobjekt
- Anforderungen
- Maßnahmen
- Zeitrahmen, Budget, Verantwortung

Verfahrensmaßnahme 1

Verfahrensmaßnahme 1

Verfahrensmaßnahme 1

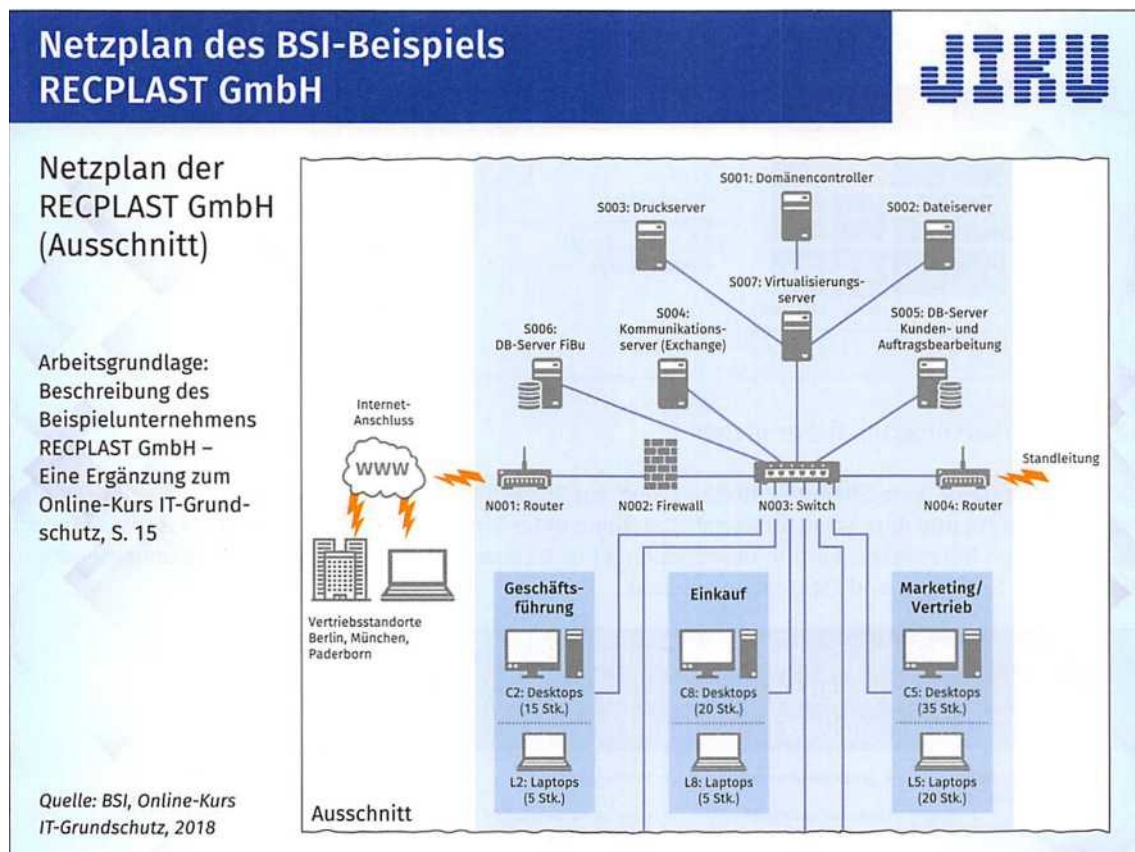
LE 2 - Netzwerkarchitektur sicher planen

Das BSI empfiehlt, eine Sicherheitsleitlinie und ein Sicherheitskonzept zu erstellen. Dazu gehören eine Strukturanalyse und eine Schutzbedarfsfeststellung unter Einbeziehung aller IT-Systeme und damit auch des gesamten Netzwerkes. Für die Bereitstellung des Netzwerkes sind Bausteine der Netzkomponenten, bestimmter Schichten und Zielobjekte genannt.



Bei den Anforderungen unterscheidet das BSI drei Kategorien, wobei die Basisanforderungen für eine grundlegende Erstabsticherung vorrangig umgesetzt werden müssen und mit geringem Aufwand den größtmöglichen Nutzen erzielen. Standardanforderungen sollten umgesetzt werden und Anforderungen bei erhöhtem Schutzbedarf je nach Notwendigkeit.

Als praktische Anleitung wurde eine Modellbeschreibung für das Modellunternehmen RECPLAST erstellt. Wie hier gezeigt, ist es sinnvoll, mithilfe eines Netzplanes alle aktiven und passiven Netzkomponenten aufzuzeigen sowie die angeschlossenen bzw. zugreifenden Clients und externen Netze.



LE 3 - Netzarchitektur und -design, technisch-organisatorische Netzwerkmaßnahmen planen

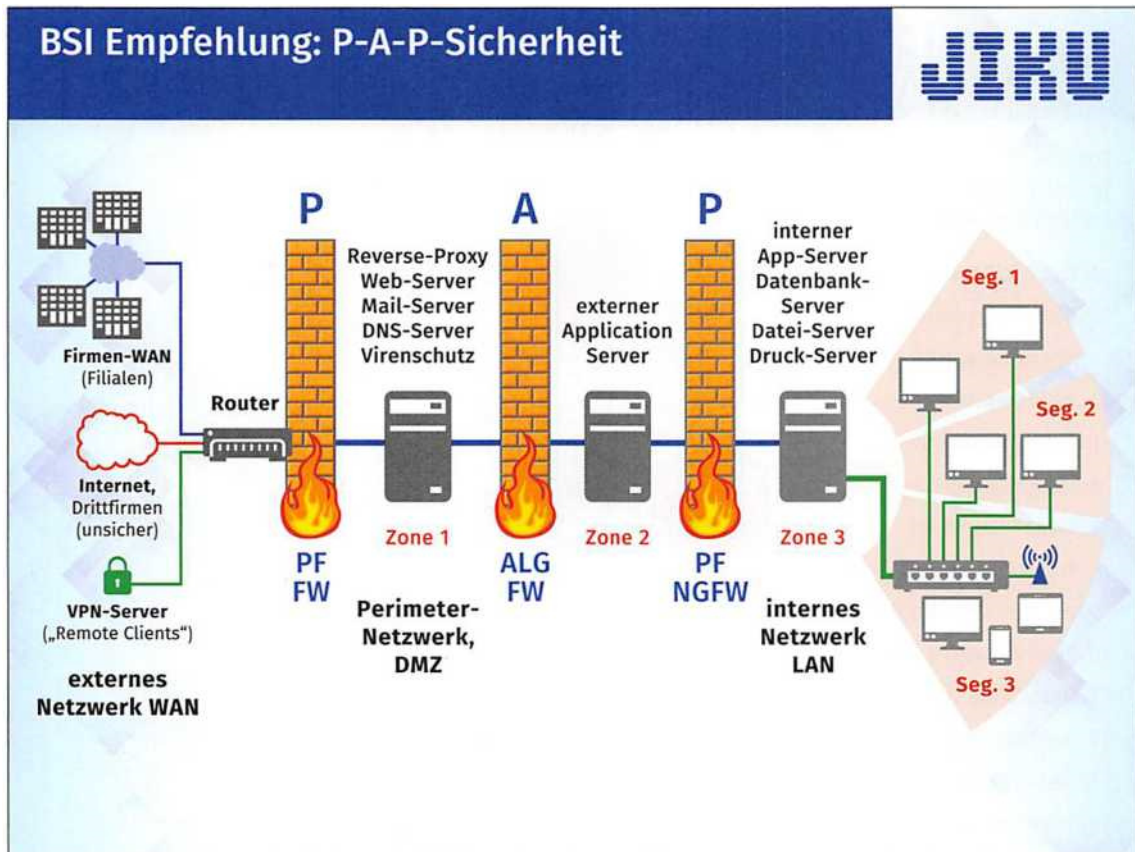
Das Bundesdatenschutzgesetz (BDSG) schreibt vor, technisch-organisatorische Maßnahmen (TOM) zum Schutz der personenbezogenen Daten im Sicherheitskonzept explizit festzulegen und ihre Umsetzung bzw. ihren Einsatz sicherzustellen.

Die Vielzahl der bezeichneten Bausteine des BSI im Zusammenhang mit Netzwerken zeigt die Komplexität der Problematik und die vielen Aspekte auf, die zu planen, umzusetzen und zu prüfen sind.



Das BSI hat mit dem Baustein NET.1.1 wichtige Anforderungen an eine sichere Netzarchitektur und das Design des Netzwerkes aufgestellt. Aufgrund der unterschiedlichen Anforderungen der Unternehmen und Organisationen an die Netzwerke einerseits und an die zahlreichen unterschiedlichen Netzkomponenten und Hersteller andererseits ist es sehr schwierig, generelle Empfehlungen an die Netzarchitektur zu geben. Die Entwicklung der Netztechnologien ist derart rasant, dass für diese Grundsatzentscheidung spezielle fachliche Beratung sehr wichtig ist, hier insbesondere Anregungen für Fachgespräche und Diskussionen gegeben werden sollen.

Das BSI stellt viele Sicherheitsanforderungen an die Netzwerke. Wichtig ist dabei eine Netzwerkarchitektur, in der die Komponenten so in Sicherheitszonen bereitgestellt werden, dass sie entsprechend der Risikoanalyse wenig angreifbar und aus Sicherheitsaspekten gut managebar sind. Wenn nötig, müssen die Zonen durch eine P-A-P-Sicherheitsstruktur geschützt werden. Entsprechend müssen leistungsstarke Firewalls bis hin zur Next-Generation-Firewall mit Funktionalitäten bis in die OSI-Schicht 7 und zum Perimeterschutz eine DMZ eingerichtet werden. Sofort nach Bekanntwerden von Updates sollten aktuelle Patches eingespielt werden, laufend Antivirenschutz aktiv sein und, wenn notwendig, Verschlüsselungen vorgeschrieben sein. Ein Identitätsmanagement sollte dafür sorgen, dass nur berechtigte Personen Zugriff auf autorisierte Anwendungen und Daten haben. E-Mail-Security ist wegen der hohen Relevanz dieses Angriffsvektors besonders zu prüfen.



Elemente der Netzwerksicherheit

Antiviren-Scanner und Antiviren-Software

Antivirenschutz ist heute Standard in jedem Unternehmen. Wichtig sind dabei eine hohe und schnelle Erkennungsrate, dazu ein großer Leistungs- und Funktionsumfang im Security Management, in der Endpoint Security, der File Server Security, Full Disk Encryption, der cloud-basierten Sandbox, der Mail Security oder der Cloud App Security.

Eine Antiviren-Software scannt jede Datei und jedes Programm, das Benutzer öffnen, und vergleicht diese mit bekannten Viren und Malware. Ein Antivirus-Scanner untersucht Programme auch nach Hinweisen auf neue, unbekannte Viren und benachrichtigt User bzw. Admin über jede verdächtige Aktivität.

Patches und Updates

Softwareentwickler entdecken fast täglich neue Schwachstellen und Sicherheitslücken, bieten daher Sicherheitsupdates (Korrekturlieferungen) an. Admins sind aufgefordert, die Software tagesaktuell zu halten, um bei verfügbaren Updates die entdeckten Schwachstellen möglichst bald zu schließen.

HTTPS bzw. Sicherheitszertifikate für die Websites einrichten und prüfen

Es ist wichtig, dass Kunden auf sichere Unternehmensseiten zugreifen können. Dazu müssen die Unternehmen für ihre Domains SSL/TLS-Sicherheitszertifikate über eine Zertifizierungsstelle des Web-Providers beziehen (bzw. über die offene Zertifizierungsstelle www.letsencrypt.org kostenlos) und einrichten. Bei Einsatz von SSL/TLS werden die Daten der Webseite verschlüsselt übertragen, erkennbar am https bzw. Schloss an der Domain.

VPN und Verschlüsselung

Für die Perimeter-Sicherheit können auch Virtual Private Networks (VPN) einen entscheidenden Beitrag leisten. VPN sind in sich geschlossene, logische Netze auf unterschiedlichen Schichten des OSI-Referenzmodells, je nachdem welche Benutzergruppen betroffen sind. Sie arbeiten auf den unteren Schichten und verwenden Tunneling für den IP-Datenverkehr.

Ein vorgeschalteter Reverse-Proxy (s.o.) kann eingehende Anfragen auf mehrere Server verteilen, Virens Scanner oder Paketfilter verwalten und damit Server im Hintergrund zusätzlich absichern. Ein Proxy-Server ist damit ein wichtiges Element in der Sicherheitskette zwischen dem Internet und dem internen Netzwerk. Zusätzlich wird ein Reverse-Proxy-Server in der Kommunikationsschnittstelle zur Verschlüsselung eingesetzt. Der Proxy dient der Auslagerung der SSL- Zertifikate und entlastet den Webserver.

Netzwerksegmentierung und P-A-P-Struktur

Eine Klassifizierung und Segmentierung des Unternehmensnetzwerks nach Vertrauenszonen und Sicherheitsrichtlinien ermöglicht für Benutzer eingegrenzte Zugriffe, verkleinert die Angriffsfläche für Bedrohungen und vereinfacht die Zugriffskontrolle. Das BSI hebt als Basis der Spezifikationen von Netzarchitektur und Netzdesign die Erstellung eines umfassenden Segmentierungskonzepts für das interne Netz hervor. IT-Systeme mit unterschiedlichem Schutzbedarf sollten in verschiedenen Netzsegmenten platziert werden, der Schutzbedarf sich nach dem höchsten vorkommenden Schutzbedarf im Netzsegment richten. Darüber hinaus sollten die Netzsegmente abhängig von ihrer Größe und den Anforderungen des Segmentierungskonzepts weiter unterteilt werden. Es muss nach dem BSI sichergestellt sein, dass keine Überbrückung von Netzsegmenten oder gar Zonen möglich ist. In Netzsegmenten, insbesondere bei IPv6 gut möglich, sollten nur Clients angebunden werden, deren Anforderungsprofile hinreichend ähnlich sind und die insbesondere denselben Schutzbedarf besitzen. Das Prinzip der kleinen Netze sollte beachtet werden. Gehören virtuelle LANs (VLANs) an einem Switch unterschiedlichen Institutionen an, sollte die Trennung physisch erfolgen.

P-A-P-Struktur: Wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation für ein Netzsegment besondere Sicherheitsanforderungen stellt, wird vom BSI eine P-A-P-Struktur gefordert, die aus Paketfilter, Application Layer Gateway (ALG) bzw. Sicherheits-Proxys und Paketfilter besteht (siehe oben). Das betriebliche Netz sollte über eine Firewall mit P-A-P- Struktur an das Internet angeschlossen werden. Zwischen den beiden Firewall-Stufen muss nach dem BSI ein proxy-basiertes ALG realisiert werden. Die interne Firewall muss die Angriffsfläche des ALGs oder der Sicherheits-Proxys gegenüber Innentätern oder IT-Systemen im internen Netz reduzieren.

Perimetersicherheit: Dies wird als die Sicherheitsgrenze bzw. der Sicherheitsbereich zwischen einem öffentlichen Netz bzw. Internet und einem Privatnetz oder internem Unternehmensnetz verstanden, um das interne Netz zu schützen. Sie wird durch Perimeter-Firewalls und VPNs realisiert, die eine erste Verteidigungslinie zum Schutz des eigenen Netzwerks gegen Viren, Würmer, Trojaner, Hacker und andere Angriffe bilden. Dazu können in weiteren Sicherheitslevels Sicherheitstechnologien wie Virens Scanner, Antiviren-Software und Webfilter eingerichtet werden.

DMZ (Demilitarized Zone = Entmilitarisierte Zone): Ein aus Sicherheitsgründen eingerichtetes eigenes Netz bzw. Netzsegment, das an Netzübergängen gebildet wird und sowohl von innen als auch von außen erreichbar ist. Die DMZ ist weniger stark gesichert als das interne Netz, dafür aber besser vom äußeren Netz aus erreichbar. Sie dient der Schaffung eines zusätzlichen Sicherheitsbereichs für öffentlich zugängliche Server/Dienste (z. B. E-Mail, Web) oder Proxys, die von externen Netzen aus nutzbar sein sollen, aber aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen. Wird ein Server in der DMZ kompromittiert, d.h. der Zugriff auf geheime, verschlüsselte Daten und die Serverkontrolle erlangt, evtl. Systeme und Daten manipuliert, so schützt die interne Firewall das interne Netz weiterhin.

Firewalls

Firewalls sind Gatekeeper, die in verschiedenen Arten den Datenverkehr nach vorgegebenen Regeln durchlassen/unterbinden und zwischen dem Netzwerk eines Unternehmens und externen, nicht vertrauenswürdigen Netzwerken eingerichtet sind.

Firewalls werden derzeit in mehreren Generationen angeboten und filtern in verschiedenen OSI-Schichten: Ein Paketfilter greift nach diesem Schichtenmodell auf die OSI-Schicht 3 (IP-Adresse) und 4 (Port) aus den Header-Informationen eines Netzwerkpaketes zu, eine Proxy Firewall oder eine Firewall mit Stateful Inspection (zustandsgesteuerte Filterung) ggf. auch auf Schicht 7 (Nutzdaten, Anwendungsschicht), NGFW grundsätzlich bis zur OSI-Schicht 7.

Firewall-Arten: Personal Firewall (auch Desktop-Firewall als Software), externe Firewall (auch Netzwerk- oder Hardware-Firewall genannt), mit erweiterten Funktionen die NGFW.

Next-Generation Firewall (NGFW): Als Vertreter der dritten Generation sind neueste Firewall-Technologien entweder in Hardware oder Software implementiert und in der Lage, ausgeklügelte Angriffe zu erkennen und zu blockieren, indem sie Sicherheitsrichtlinien auf Anwendungs-, Port- und Protokollebene durchsetzen. Da es keinen Standard zur NGFW gibt, sind Funktionen genau zu vergleichen, Grundfunktionen sind z.B. Enterprise-Firewall-Fähigkeiten, ein IPS und Anwendungskontrolle. Next-Generation Firewalls sind auch besser gegen Advanced Persistent Threats (APT) gewappnet, da sie in die Threat Intelligence Services integriert werden können. Auch bieten sie i.d.R. eine Deep-Packet-Inspection-Funktion, die über eine einfache Port- und Protokollinspektion hinausgeht, indem sie die in den Netzwerkpaketen übertragenen Daten inspiziert. Einige NGFWs unterstützen darüber hinaus die Überprüfung von TLS-/SSL-verschlüsseltem Datenverkehr, Webseiten-Filterung, QoS-/Bandbreiten-Management, Virenschutzprüfung und Integration mit Identitätsmanagementsystemen von Drittanbietern wie LDAP, RADIUS und Active Directory, siehe Empfehlung des BSI zu NGFW (BFI-CS 112).

Zwei Firewalls: Die sicherste Methode ist die Verwendung von zwei Firewalls, um damit eine DMZ einzurichten. Die erste Firewall (Frontend- oder Perimeter-Firewall) wird so konfiguriert, dass nur der Datenzugriff für die DMZ erlaubt wird. Die zweite Firewall (Backend-Firewall) erlaubt nur Datenzugriffe, die von der DMZ das Regelwerk ins interne Netzwerk erfüllen. Um den internen Netzschutz weiter zu erhöhen, wird die Verwendung von Firewalls von verschiedenen Anbietern empfohlen, da die Wahrscheinlichkeit dann geringer ist, dass diese die gleichen Sicherheitslücken aufweisen.

UTM-Firewalls (Unified Thread Management): Für Sicherheitsservices werden NGFW oder UTM-Lösungen (Unified Thread Management) als Desktop-Geräte, Rackmount-Lösungen oder cloud-basierte Appliances angeboten. Aufgrund fehlender Standards hat sich eine Durchmischung ergeben, sind Appliances je nach Leistungsanforderungen daher genau zu vergleichen. UTM-Appliances enthalten i.d.R. gebrauchsfertige Richtlinien, Verwaltungs- und Reportingtools für die einfache Bereitstellung und laufende Verwaltung. NGFW-Appliances sind besonders für Unternehmen geschaffen, die ihre Sicherheitsrichtlinien kundenspezifisch anpassen möchten und manuelle Reporting- und Managementtechniken bevorzugen. UTM-Firewalls stellen i.d.R. Funktionen wie Anti-Virus, Anti-Spyware, Anti-Spam, Netzwerk-Firewall-Funktionen, Angriffserkennung und -Überwachung, Inhaltsfilter und das Verhindern von Datenlecks bereit, evtl. zusätzlich Remote-Routing, Übersetzung von Netzwerkadressen (NAT) und Unterstützung für virtuelle private Netzwerke (VPN).

Paketfilter: In der Grundfunktion des Softwaremoduls erfolgt die einfache Filterung (Ports und der IP-Adresse des Quell- und Zielsystems) von Datenpaketen anhand von Filterregeln. Unzulässige Pakete werden verworfen (DENY oder DROP), als unzulässig (REJECT) erklärt oder weitergeleitet (FORWARD oder PERMIT) beziehungsweise durchgelassen (ALLOW oder PASS).

Proxyfilter: Er stellt die Verbindung mit dem Zielsystem her und leitet die Antwort des Zielsystems an den tatsächlichen Client weiter.

Content-Filter: Er wertet als Proxyfilter die Nutzdaten einer Verbindung aus, blockiert oder sperrt das Weiterleiten.

„Intrusion Detection Systeme" (IDS) und „Intrusion Prevention Systeme" (IPS): Sie erkennen einen Einbruchversuch anhand von Kommunikationsmustern. IDS erkennt nur den Angriff und IPS wird den erkannten Angriff auch blockieren.

Firewall-Regelwerk: Es legt fest, wie mit Netzwerkpaketen zu verfahren ist, z. B. verwerfen (DROP), aktiv ablehnen (REJECT), erlauben (ACCEPT, PASS, FORWARD).

Weitere Funktionen sind:

Application-, Web- und Inhaltskontrolle: Content-, Spam-Filter, Antiviren-Filter, Richtlinien- Management

E-Mail und Datenschutz: Datenverkehrskontrolle etc.

Web-Protection: Web-Bedrohungen erkennen und beseitigen

Advanced Thread Protection: erkennt Bots und komplexe Bedrohungen

Deep Packet Inspection: Verfahren der Netzwerktechnik und von Firewalls, um Datenpakete sowohl zum Header als auch zum Dateninhalt zu überwachen und zu filtern, dabei weitgehende, besonders protokollspezifische Informationen analysiert. Mit SSL Deep Packet Inspection können verschlüsselte Verbindungsdaten und Inhalte entschlüsselt und anschließend für den Client wieder neu verschlüsselt werden.

Zero-Day- und KI-Schutz, Sandboxverfahren: Erkennung neuester Bedrohungen schnellstmöglich mit Maschine Learning und Schutz durch Sandboxing.

Benutzeridentitätsmanagement: Zugriff nur autorisierter Personen auf Anwendungen und Programme, zusätzlich Anwendungsbeschleunigung durch Richtlinienmanagement und Bandbreitenmanagement.

Sicherheits-Gateway: Für normalen Schutzbedarf besteht es im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application Level Gateway (ALG) zu unterscheiden. Für IPv4 stellen Paketfilter bedarfsweise die Funktion „Network Address Translation" (NAT) zur Verfügung. Für IPv6 übernehmen diese Aufgabe implizit die ALGs. Dazu kommen noch Port Address Translation (PAT) und URL-Blockierung.

E-Mail-Sicherheit

E-Mail ist einer der am meisten eingesetzten Angriffsvektoren, daher ist der Schutz vor E-Mail- Bedrohungen wie Phishing, Ransomware, Business-E-Mail-Compromise-Angriffen (BEC) sehr wichtig. Manipulationssichere E-Mail-Archivierung ist zur Sicherstellung von Compliance-Vorgaben wichtig. Bei E-Mail-Programmen ist darauf zu achten, dass Übertragungsprotokolle (POP3S, IMAPS, SMTPS) verwendet werden. Unternehmen richten dazu E-Mail-Security-Gateways ein, die Angriffe blockieren oder unsichere Inhalte in Quarantäne verschieben. Sie werden auf dem E-Mail-Server installiert, als Hardware-Appliance (Geräte- und Lizenzkosten) oder virtuelle Appliance (Abonnementkosten) eingerichtet.

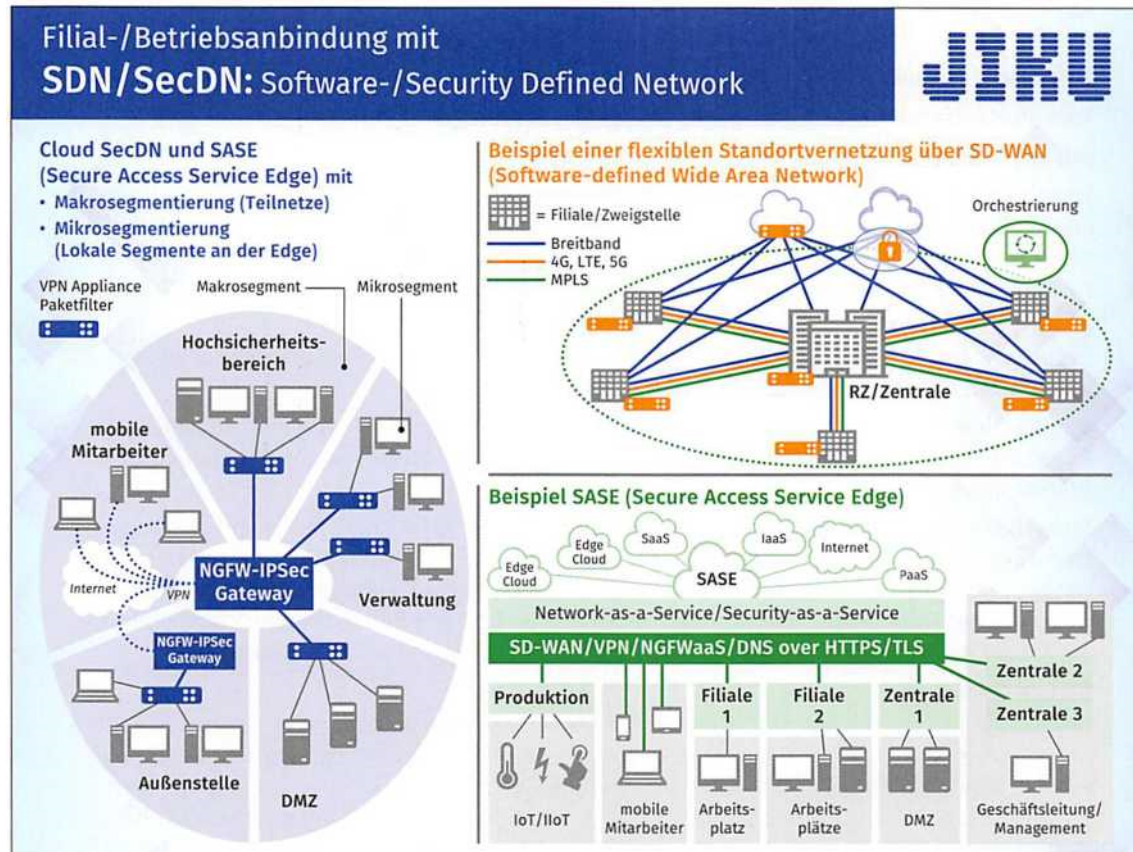
Der Spamfilter stellt zur Filterung von E-Mail-Absendern die Eintragung in eine Blacklist oder eine Whitelist zur Verfügung. Eine Blacklist ist eine Liste von unerwünschten Absendern (Domains oder Mailboxen), die abgewiesen werden sollen (reject, deny, drop), alle anderen werden weitergeleitet. Bei Einsatz einer Whitelist werden erwünschte Absender weitergeleitet (accepted), alle anderen Absender zurückgewiesen.

LE 4 - Cloud-, Filial- und Betriebsanbindungen über Software Defined Networking

Software Defined Networking (SDN) ist ein Netzwerkkonzept, das die zentrale, intelligente Verwaltung und Steuerung der einzelnen Hardware-Komponenten mithilfe von Software ermöglicht. Der Einsatz offener Protokolle wie "OpenFlow" ermöglicht dabei den zentralen Zugriff auf Netzwerkgeräte wie Switches, Router oder Firewalls. Geräte klassischer Netzwerksicherheit stoßen in komplexen Netzwerken zunehmend an Grenzen, sodass besonders hier Architekturen in Richtung Cloud und Software Defined Networking (SDN) umgesetzt werden. Vorteile werden

hier in einer größeren Verfügbarkeit bei geringeren Leitungskosten und auch in einer größeren Vertraulichkeit der Daten gesehen. In SDN-Systemen kann Sicherheit einerseits zentral gemanagt werden, andererseits von Fachabteilungen durch Management vor Ort bzw. an der Edge durch eigene, passende Sicherheitsregeln verbessert werden.

Die Sicherheitsinfrastruktur wird in der Basis über Makrosegmente (klassische Teilnetze) und dezentral eingerichtete Mikrosegmente unterteilt, die lokal verantwortet werden. Je nach Anbieter bzw. Betreiber und verwendetem Kommunikationsstandard variieren die Vorstellungen und Ansätze zur Umsetzung von SDN-Strukturen.



Zero-Trust-Sicherheitsprinzip und -Software/Security Defined Networking

Zero-Trust-Sicherheitsprinzip, -Methode oder -Architektur

Zero Trust ist ein IT-Sicherheitsmodell, welches das Was (Daten, Anwendungen, Ressourcen, Dienste) auf Mikroperimeterebene (Layer-7-Richtlinien) als die zu schützende Angriffsfläche fokussiert und nicht die gesamte Angriffsfläche (Makroperimeter des Systems). Dazu gehören Netzwerksegmentierung und strenge Zugriffskontrollen. Umgesetzt wird dies durch den Einsatz von Firewalls der nächsten Generation (Next-Generation Firewall, NGFW), die auch als Segmentierungs-Gateways bezeichnet werden und nur bekannten Datenverkehr von legitimen Anwendern und Anwendungen zulassen. Eine NGFW bietet Transparenz im Datenverkehr und setzt die Zugriffssteuerung anhand der Kipling-Methode durch (Zugriffsrichtlinien auf Basis von Wer, Was, Wann, Wo, Warum und Wie definiert.).

Die Zero-Trust-Architektur wird nach einer Fünf- Schritte-Methode bereitgestellt und betrieben:

- Schutzoberfläche einschließlich sensibler Daten und Anwendungen als „öffentlich“, „intern“ oder „vertraulich“ identifizieren
- Transaktionsflüsse aller sensiblen Daten zwischen Personen und Anwendungen intern/extern feststellen und optimieren

- Zero-Trust-Architektur/-Design entwickeln, z. B. über Sicherheitsprotokolle, NGFW, NSX und/ oder Software-Defined-Netzwerken oder Data-Centers (SDDC)
 - Zero-Trust-Richtlinien nach der Kipling-Methode erstellen
- Automatisierung, Überwachung und Wartung sicherstellen, um alle Aktivitäten und Datenflüsse zu überwachen

Software Defined Networking (SDN)

Es ist ein Netzkonzept, das Hard- und Software entkoppelt und die Netzkomponenten zentral verwaltet. Die Hardware selbst ist nur noch für die reine Weiterleitung der Datenpakete verantwortlich und besitzt selbst keine eigene Intelligenz. Die Geräte arbeiten auf Layer 3 oder Layer 2 und führen auf Datenebene die Aufgaben von Routern oder Switches aus. Die beiden zentralen Komponenten eines SDN sind die Control Plane und die Data Plane. Die Data Plane führt die Anweisungen der Control Plane aus. Dies können beispielsweise die Regeln für das Routing der Datenpakete sein. Der Network-Controller ist das zentrale Steuerungselement im Netzwerk und kann eine Vielzahl verschiedener Netzwerkkomponenten wie Router oder Switches steuern und verwalten. Das Netzwerkbetriebssystem verarbeitet und speichert alle für die Steuerung und das Management benötigten Informationen. Ein wesentlicher Vorteil des Software-Defined Networkings ist, dass das Netzwerk sehr flexibel erweiterbar, änderbar und managebar ist, wegen der Trennung von Hardware und Software grundsätzlich keine Abhängigkeiten zu den Geräteherstellern entstehen sollten. Große Netzkomponenten- Hersteller haben auch die Vorteile von SDN erkannt und bieten auch dafür eigene Lösungen an. Mit OpenFlow steht ein offenes Protokoll für dynamisches und komplexes Management zur Verfügung. Das Southbound-Interface stellt die Kommunikation zwischen Control und Data Plane her, kommuniziert nach unten mit tieferen OSI-Schichten, bzw. Komponenten (Router, Switches, u.a.), des Netzwerks und das Northbound-Interface mit höheren Ebenen der Applikationen, Management- und Kontrollprogramme. So finden über dieses Interface Automatisierung und Orchestrierung statt.

Bedrohungsscanner, OpenVAS und Surity Manager einsetzen

Security- oder Vulnerability-Scanner sind Computerprogramme und Dienste, die Zielsysteme auf das Vorhandensein von bekannten Sicherheitslücken hin untersuchen, mit "OpenVAS" wird ein Open-Vulnerability-Assessment-System eingesetzt. Schwachstellen-Management (Vulnerability Management, VM) dient einer proaktiven Asset-Erfassung, kontinuierlichem Monitoring, der Eindämmung, Behebung und Verteidigung von Cyberangriffen.

Sicherheits-Gateway als SaaS, Secure Access Service Edge (SASE)

Für Cloud-Netze wehren Secure Web Gateways gezielte Bedrohungen wie Malware oder Ransomware ab. Es werden DNS-Datenextraktionen, Zero-Day-Angriffe auf mobile Geräte proaktiv erkannt, blockiert bzw. eingeschränkt. Mit SASE werden gesicherte Netzverbindungen zu Cloud- Diensten hergestellt. SASE für Secure Access Service Edge beschreibt ein Cloud-Architektur- modell, das Netzwerk- und Security-as-a-Service-Funktionen bündelt und als einen gemeinsamen Cloud-Service bereitstellt. Netz- und Sicherheitsfunktionen können unabhängig von jedem Ort im Netz verwaltet werden, sodass verteiltes Sicherheitscontrolling, verteiltes Richtlinienmanagement sowie schnelle Erweiterung der Ressourcen möglich sind.

Security-Information-and-Event-Management-Systeme (SIEM)

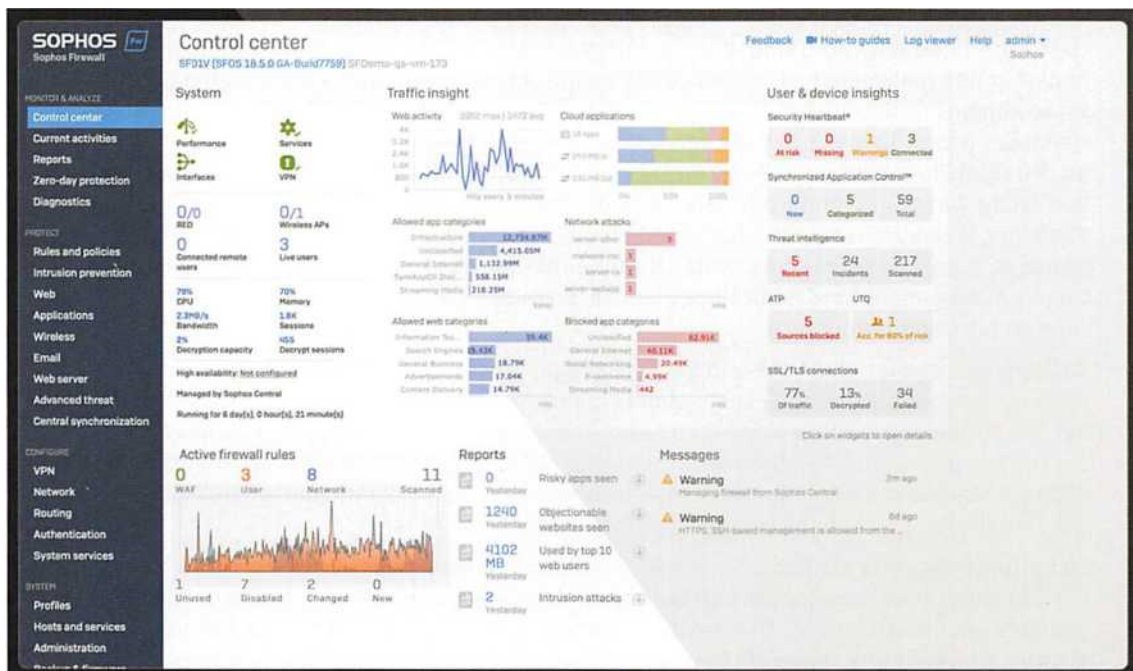
Sicherheitsbeauftragte und Security Operation Center (SOCs) von Unternehmen setzen immer mehr SIEM-Systeme ein, um die Sicherheitslage mit mehreren hundert schweren Bedrohungen pro Tag auf das Unternehmen zu managen. Sie analysieren in Echtzeit Datenströme, Anwendungs-, Benutzer- und Serververhalten, Log Events, bekannte Schwachstellen sowie Meldungen von Netzwerkkomponenten, dienen damit als IPS (Intrusion Prevention System) oder lösen Alarmer aus, leiten Maßnahmen ein oder unterstützen für eine schnelle Abwehr durch Reports oder Log-Informationen.

Durch die Anbindung an Wissensdatenbanken werden aktuelle Informationen für die Gefahrenabwehr bereitgestellt. Insbesondere SIEM-Systeme, die Machine Learning, UEBA (User and Entity Behavior Analytics) und SOR (Security Orchestration, Automation and Response) nutzen, können Sicherheitsmanager effektiv entlasten.

Netzwerksegmentierung

Netzwerksegmentierung erfolgt in Software Defined Networks auf lokaler Microebene (Layer-7- Ebene). Eine Klassifizierung und Segmentierung des Unternehmensnetzwerks nach Vertrauenszonen und Sicherheitsrichtlinien ermöglicht für Benutzer eingegrenzte Zugriffe, verkleinert die Angriffsfläche für Bedrohungen, vereinfacht die Zugriffskontrolle und optimiert die Compliance.

Zur Bereitstellung eines sicheren Netzwerkes gehört auch die Installation eines umfassenden und leicht zu managenden Sicherheitsmanagementsystems. Im Beispiel (siehe Screenshot) wird das Dashboard des Control-Centers von Sophos gezeigt. Damit ist es möglich, alle Devices oder eine Firewall des Netzwerks sicherheitsrelevant zu managen, den Sicherheitsstatus anzuzeigen, auftretende Warnungen (Alerts) zu bearbeiten, Computer manuell oder automatisch von Malware zu bereinigen. Im Device Control können Gerätesteuerungsfunktionen (z.B. Geräte sperren) genutzt werden, es können Benachrichtigungen an Nutzer verfasst werden oder Reports erstellt werden.



Optik des Control-Centers von Sophos, ein britisches Unternehmen für Sicherheitssoftware

Nicht zuletzt sind die Endpoints im Sicherheitskonzept besonders zu berücksichtigen und hierbei sichere Authentifizierung der Benutzer, die Installation von End-Point-Protection-Suites, VPN oder Verschlüsselungstools zu berücksichtigen sowie nicht zuletzt alle Mitarbeiter in der Gefahrenabwehr durch Social Engineering zu schulen.

Endpoint- bzw. Enduser-Security

Multi-Faktor-Authentifizierung oder Single-Sign-on (SSO)

Einsatz sicherer Anmelde- und Berechtigungssysteme, um die Identität der Mitarbeiter schnell zu überprüfen und über ein Access Management (IAM) auf notwendige Ressourcen zugreifen zu können. Eingesetzt werden können biometrische Merkmale, Token oder Smart Cards. Zero Trust ist eine ganzheitliche Strategie mit entsprechenden Produkten und Lösungen, die bei der Authentifizierung ansetzt.

Endpoint-Protection-Suite-Pro

Installation einer leistungsstarken Antiviren-Software bzw. Endpoint-Security-Apps, um Angriffe abzuwehren

VPN (Virtual Private Network)

Über eine geschützte Netzwerkverbindung wird der Datenverkehr durch einen in Echtzeit verschlüsselten virtuellen Tunnel geleitet, die IP-Adresse und damit die Online-Identität werden verschleiert. Dabei wird ein speziell konfigurierter VPN-Server (oder VPN-Anbieter) verwendet. Es gibt verschiedene Arten von VPN (z. B. SSL-VPN, Site-to-Site VPN, Client-to-Server-VPN). VPN schützt nicht davor, dass Daten auf Endgeräten geschädigt oder ausgespäht werden.

Social-Engineering und Zero-Trust-Strategie

Es ist wichtig, Endbenutzer auf ihre Vertraulichkeitspflichten im Umgang mit den Geräten, Passwörtern und Anwendungen zu sensibilisieren und zu informieren. Wenn möglich, sind dazu Zero-Trust-Anwendungen einzusetzen.

Nur sichere Seiten aufrufen: Browser zeigen bei sicheren Webseiten ein Schlosssymbol neben der URL an bzw. ein „https“ statt einem „http“ in der Domainanzeige für ein sicheres Kommunikationsprotokoll. Damit wird angezeigt, dass die Webseite über ein SSL/TLS-Sicherheitszertifikat verfügt, die die sichere und verschlüsselte Verbindung zur Webseite bestätigt.

Verschlüsselung vertraulicher Dateien und E-Mails

Siehe Module „Clients im Netzwerk einrichten“ und „Schutzbedarfsanalyse“

LE 5 - Nachhaltigkeit sicherstellen

Viele Milliarden Kilowattstunden Strom benötigen Netzwerke und Services, die heute in der IT genutzt werden. Schätzungsweise 20 bis 50 Millionen Tonnen Elektroschrott werden weltweit jedes Jahr entsorgt. Schwermetalle und andere gefährliche Stoffe landen auf den Deponien. Rechenzentren benötigen heute über 3% der weltweiten Stromversorgung und verursachen über 2% der globalen Treibhausgasemissionen.

Immer häufiger werden beispielsweise zusätzliche Graphics Processing Units (GPUs) eingesetzt, um die Leistung der Systeme zu steigern. Die jüngste Generation an GPUs hat dabei eine Leistungsaufnahme von bis zu ca. 400 Watt. Für einen leistungsfähigen Server kommen so in einer Musterrechnung schnell 2 500 Watt Leistungsaufnahme zustande (bei zwei CPUs à 300 Watt, vier GPUs à 400 Watt sowie Arbeitsspeicher, NVMe-Speicher und Netzwerkadapter). In einem herkömmlichen 19-Zoll-Rack mit 42 Höheneinheiten finden bis zu 36 solcher Server Platz. Das entspricht einer Leistungsaufnahme von bis zu 90000 Watt pro Rack. Mit der Leistungssteigerung erhöht sich die Wärmeabgabe. Da die Leistung der CPUs und GPUs auch von der Temperatur abhängt, muss für eine Kühlung gesorgt werden. Es muss daher besonders nach Neuerungen gesucht werden, die Entwicklungen zu immer höherem Stromverbrauch stoppen. Nachhaltigkeit und Green-IT sind zu einem wichtigen Thema der IT geworden, in vorherigen Modulen wurde diese Problematik bereits thematisiert.

Zu Green-IT gibt es viele Initiativen, die sich um eine Verbesserung der Ökobilanz in der IT bemühen. Unternehmen verpflichten sich mit der ISO 14001 und ISO 14004, über ein Nachhaltigkeitsmanagement stetige Fortschritte zu erzielen, jährlich in Nachhaltigkeitsberichten ihre Fortschritte den Stakeholdern nachzuweisen. Corporate Social Responsibility (CSR) ist vielen Unternehmen wichtig.



ISO 14001 und ISO 14004

Umweltmanagementsysteme (ISO 14001) und Allgemeine Leitlinien zur Verwirklichung (ISO 14004)

Die ISO 14001 ist der weltweit akzeptierte und angewendete Standard für Umweltmanagementsysteme, zuletzt im Jahr 2015 novelliert. Unternehmen lassen sich weltweit nach dieser Norm zertifizieren. Zur Hilfestellung stehen mit der Norm ISO 14004 Leitlinien mit Erläuterungen und Hilfestellungen bereit.

CO₂-Bilanz und CO₂-Zertifikate

Auf der Basis von UN-Vereinbarungen und des Kyoto-Protokolls sowie Nachfolge-Klimakonferenzen haben sich Staaten auf Klimaziele und Klimaschutzmaßnahmen geeinigt. Um die Schadstoffemissionen zu senken und Klimaziele zu erreichen, werden u.a. Unternehmen und Verbraucher durch CO₂-Abgaben und CO₂-Zertifikate angehalten, sparsamer mit natürlichem Ressourcenverbrauch umzugehen. Ein Zertifikat ist im Umweltrecht ein verbrieftes Recht, in einem bestimmten Zeitraum eine bestimmte Menge eines Schadstoffes zu emittieren. Immer mehr Bereiche werden per Gesetz verpflichtet, CO₂-Zertifikate für ihre Schadstoffemissionen vorzulegen und damit zu erwerben.

Umweltleitbilder

Viele Unternehmen wollen ein hohes Ansehen in Corporate Responsibility erhalten, haben für ihre Ausrichtung Leitbilder und speziell auch ein Leitbild für Nachhaltigkeit erstellt. Unternehmen mit Datacentern, Cloud-Unternehmen oder Unternehmen mit bedeutender IT-Ausstattung haben daher auch besonders hohe Ziele für hohe Umwelt- und Nachhaltigkeitsstandards gesetzt.

Nachhaltigkeits- und Selbstregulierungsinitiativen der Datacenter (RZ)

Große Datacenter-Unternehmen und Datacenter-Organisationen haben sich hohe Ziele gesetzt, Nachhaltigkeit umzusetzen. Ein Beispiel ist die Initiative „Climate Neutral Data Centre“, die sich zum Ziel für ihre RZ-Gemeinschaft gesetzt hat, Rechenzentren in Europa bis 2030 klimaneutral zu machen. Auch verpflichten sich die Unternehmen zu messbaren Zielen für 2025 und 2030 wie die Verbesserung der Energieeffizienz, Kreislaufwirtschaft, Kreislaufenergie (z. B. Nutzung von Abwärme) und Governance (www.climateneutraldatacentre.net).

Durch Disaggregation (Aufschlüsselung), z. B. der Gesamtverbrauchsdaten, und Zerlegung in kleinere Einheiten zur Ermittlung des Verbrauchs einzelner Geräteeinheiten kann die Haltbarkeit der Komponenten und damit der Aktualisierungszyklus ermittelt werden.

Maßnahmenkatalog zur Nachhaltigkeit in Rechenzentren und IT-Netzwerken

Stromverbrauchsreduzierung

Der Energiebedarf im Datacenter/RZ ist durch den Stromverbrauch von Servern, Speichern und Netzen erheblich. Eine der wichtigsten Kennzahlen zur Berechnung des effizienten Energieverbrauchs ist der Effizienzwert „PUE“ (Power Usage Effectiveness). Er setzt die Gesamtenergie, die eine Rechenzentrumseinrichtung verbraucht, ins Verhältnis zu der Energie, die an die IT- Ausrüstung geliefert wird. Die Werte bewegen sich zwischen 1,6 und 2, der Optimalwert liegt derzeit ca. bei 1,1.

Maßnahmen sind die Optimierung der bestehenden Stromverteilung im Rechenzentrum, der Einsatz stromsparender Geräte, die Reduktion des Stromverbrauchs durch Leitungen, die Stromverbrauchssenkung durch Virtualisierung, eine bessere Klimatisierung bzw. der Einsatz klimaresistenterer Geräte etc.

Kühlung/Klimaanlage

Die Klimatisierung von Datacentern hat häufig einen hohen Strombedarf. Es werden daher effizientere Kühlsysteme (z. B. Warmwasserkühlung) eingesetzt. Es gibt mittlerweile Rechenzentren, die keine Klimaanlage mehr benötigen oder den Einsatz einer Klimaanlage auf ein Minimum reduziert haben, Systeme einsetzen, die bis zu ca. 45°C Temperatur aushalten. Im Winter wird die Wärme zur Gebäudebeheizung verwendet. Eine saubere Verkabelung der Anschlüsse am Server trägt außerdem zu einer besseren Verteilung der Kühlluft bei, sodass Lüftungen im Server langsamer laufen können. Durch Verblindungen für freie Höheneinheiten (HE) in Racks wird eine verbesserte Kaltluft-Leitung und damit wertvolle Energie eingespart (Kalt-/Warmgangeinhausung).

Ressourcenreduktion Hardware

Um den Elektroschrott und die damit verbundenen Schadstoffe sowie den Verbrauch seltener Erden einzudämmen, sind viele Maßnahmen möglich:

- Refurbishing, Recycling und Remarketing von Altgeräten
- Einsatz effizienterer Hardware
- Schwere und Heavy-Load Server sollten in der Nähe der Lüftungsausgänge platziert werden.
- Server, die nicht aktiv genutzt werden, verbrauchen eventuell zu viel Strom (ca. 40% eines unter Last laufenden Servers) und sollten gemanagt heruntergefahren werden.
- Ressourcenschonung durch Virtualisierung
- Statt Netzteilen in den Servern werden die einzelnen Trays (bzw. Server) direkt von einem zentralen großen Netzteil im Rack mit Gleichstrom versorgt.
- Multinode-Server und höhere Leistungsdichten können die Energie-Anforderungen drastisch verbessern und außerdem Kosten senken.

Ressourcen-Reduktion Software

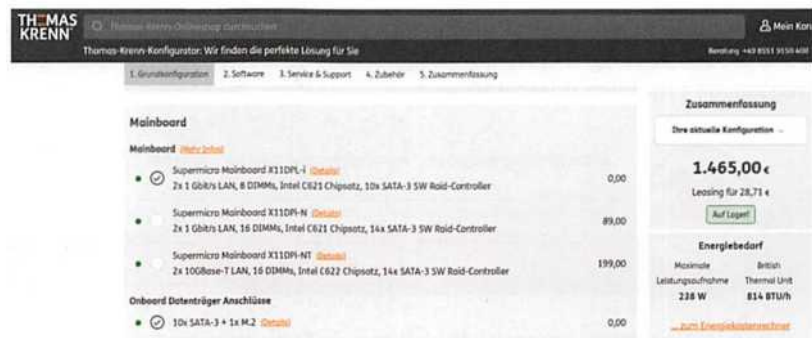
Software sollte so entwickelt werden, dass Geräteressourcen und Leistungen stromsparend eingesetzt werden. Eine Reduzierung der Datenkommunikation in Cloudsystemen und damit Energieeinsparungen sind durch den Einsatz von Edge- und Fog-Technologien möglich.

TAG 12 - Pflichtenhefte nach Unternehmensanforderungen erstellen

Die folgenden Kapitel bauen auf die gelegten Grundlagen auf und konkretisieren weiter die Verfahren zur Beschaffung und Bereitstellung von Netzwerktechnik. Hierbei werden zunächst digitale Beschaffungsplattformen dargestellt, um Möglichkeiten für eigene Recherchen zu eröffnen und professionelle Beschaffungswege aufzuzeigen. Pflichtenhefte werden auf Ausschreibungsplattformen als Leistungsbeschreibungen veröffentlicht. Es wird auf diese Plattformen eingegangen und damit gezeigt, wie Unternehmen und öffentliche Einrichtungen diese kommunizieren. Nach Darstellung der Ausschreibungs- und Vergabeplanung mit der Kurzvorstellung der Beispielaufträge werden passend zu den Aufträgen ausgewählte funktionale und nicht funktionale Anforderungen näher behandelt.

LE 1 - Ausschreibungs- und Vergabeplanung

Die meisten Beschaffungs- und Bereitstellungsprojekte scheitern, wenn Vergaben an mögliche Auftragnehmer nicht gut geregelt sind, sodass zwischen Auftraggebern und Auftragnehmern Unstimmigkeiten und Ablaufprobleme entstehen. Um ein geordnetes und geregeltes Verfahren sicherzustellen, werden von den Auftraggebern möglichst genaue Verfahrensregeln vorgegeben. Für Beschaffungsmaßnahmen öffentlicher Maßnahmenträger sind Gesetze und Verordnungen sowie strenge Regeln für das Vergabeverfahren von Aufträgen zu beachten. Großunternehmen haben i.d.R. vergleichbare Vergabeverfahren für ihre Beschaffungsmaßnahmen festgelegt und auch kleinere Unternehmen berücksichtigen bei Beschaffungsverfahren Methoden, die sich bei öffentlichen Unternehmen bewährt haben und eine erfolgreiche Beschaffung und Bereitstellung gewährleisten. Wo viel Geld im Verfahren ist, werden heute strenge Compliance-Regeln gefordert, um Korruption (Missbrauch einer Vertrauensstellung), Kollusion (unerlaubtes Zusammenwirken mehrerer Beteiligter) und sogenannter Vetternwirtschaft entgegenzuwirken.



Um Leistungsbeschreibungen zu erstellen, werden Leistungswerte (KPI) über Internetplattformen der Hersteller oder Internetshops ermittelt und bei den Leistungsbeschreibungen berücksichtigt. Speziell für IT-Produkte stehen hunderte von Angeboten im Internet zur Auswahl. Einige bieten Konfiguratoren auch für Netzwerkprodukte (z. B. Server) nach dem BTO-Prinzip (Build-to-Order) an, dazu noch viele unterstützende Services für gewerbliche bzw. nicht private Kunden. Einkäufer und Beschaffer finden schnell Lieferanten über Lieferantenportale. Unabhängige digitale Beschaffungsportale bringen Lieferanten und Kunden zusammen und organisieren insbesondere für Standardartikel eine einfache Beschaffungslogistik einschließlich des Bezahl- und Retourenprozesses.

Internetshops, Marktplatz- und Beschaffungsplattformen, Lieferantensuche

Internetshops

Unternehmen beschaffen ihre IT-Komponenten häufig direkt über große Shop-Portale der Hersteller oder spezialisierter IT-Anbieter, da sie auf hochwertige Systeme und Komponenten für die Unternehmensverwendung, Beratung, Unterstützung, Bereitstellungs- und Wartungsservice großen Wert legen. Da Computersysteme und Server speziell nach den Anforderungen konfiguriert werden müssen, bieten sie in den Shops digitale Konfiguratoren an (Build-to-order-Prinzip, BTO, Fertigung nach Auftrag). Verschiedene Plattformen ermitteln jährlich ihre besten Wiederverkäufer (Distributoren, Value-added Reseller) und die Rankings. Große IT-Systemhaus-Unternehmen bieten über das Internet standardisierte und individuelle Services an.

Lieferantensuchportale

Um Anbieter oder Lieferanten schnell zu finden und schnell allgemeine und qualifizierte Anfragen zu erstellen, bieten sich sogenannte Lieferantensuchportale an.

B2B-Marktplätze

Als unabhängige digitale Marktplätze haben sich Dienstleistungsunternehmen etabliert, die über ihre Plattformen Unternehmen im gewerblichen Handel (B2B) unterstützen bzw. nicht private Anbieter und Kunden zusammenbringen, um ihre Leistungen anzubieten und zu kaufen. Anbieter können ihre Produkte auf den Portalen einstellen und vergleichend anbieten, Kunden können Suchanfragen stellen, Bedarfskataloge erstellen und ihre Beschaffungsorganisation für Standardartikel (i.d.R. sogenannte in kleineren Stückzahlen nachgefragte C-Artikel) optimieren und auch den Retouren- und Bezahlprozess vereinfachen.

Um Vergaben professionell zu managen, werden Ausschreibungen von öffentlichen Auftraggebern auf Ausschreibungs- bzw. Vergabeplattformen veröffentlicht. Große Unternehmen und Konzerne haben eigene Beschaffungsplattformen, um ihre großen Beschaffungsvolumina zu managen, kleinere Unternehmen vernetzen sich immer mehr mit digitalen Plattformen, um Vorteile dieser Plattformen zu nutzen.

Öffentliche Einrichtungen müssen i.d.R. ihre Aufforderungen zur Angebotsabgabe öffentlich ausschreiben und bedienen sich i.d.R. der digitalen Ausschreibungsplattformen. Die meisten dieser Plattformen bieten auch in den Kategorien IT-Systeme, Software, Lizenzen und Netzwerke schnell zu recherchierende Ausschreibungen an. Die Erfassung ist i.d.R. für die Anbieter kostenlos, die suchenden Auftragnehmer müssen für die vielfältigen Dienste z.B. monatliche Entgelte entrichten. Sind sie registriert, werden den potenziellen Auftragnehmern unaufgefordert passende Ausschreibungen angekündigt, sodass die Auftragssuche erheblich erleichtert wird.

The screenshot shows the header of the 'it ausschreibung' website. It includes a logo on the left and navigation links: 'Ausschreibung aufgeben', 'Ausschreibungen suchen', 'Anbieter', 'Infos', 'Einloggen', and 'Jetzt registrieren!'. Below the navigation is a banner with the text 'Seit 1999 die größte spezialisierte Auftragsbörse für IT- und EDV-Aufträge' and '20 JAHRE - DAS ONLINE-INFO-CENTER FÜR IT-AUSSCHREIBUNGEN'. Below the banner is a section titled 'Sie suchen IT-Ausschreibungen oder haben einen IT-Auftrag zu vergeben?' with a brief description of the service and a right-pointing arrow.

Ausschreibungsportale

Ausschreibungsplattformen bieten eine Auftragsvermittlung für Aufträge großer und kleinerer Aufträge zur Infrastrukturerstellung, Bauvorhaben, Installationsvorhaben, Dienstleistungen und mehr an. Die meisten Plattformen verwalten überwiegend Auftragsvergaben der öffentlichen Hand, andere haben auch Ausschreibungen von Unternehmen und sogar auch von Privatunternehmen in ihrer Datenbank. Es gibt auch Ausschreibungsplattformen, die sich speziell auf einen Marktbereich, z. B. den IT-Markt, ausgerichtet haben.

Ziel dieser Auftragsbörsen ist es, Auftraggeber (Beschaffer, Projektanbieter, Einkäufer) und Auftragnehmer (Anbieter von Dienstleistungen und/oder Produkten) auf einer Marktplattform zusammenzubringen. Nicht immer siegt der günstigste Preis bei der Auftragsvergabe. Oft zählen auch Qualität der angebotenen Produkte, der mögliche Liefertermin oder auch die Erfahrung bei der Ausführung einer Dienstleistung. Der Auftraggeber entscheidet für alle nachvollziehbar anhand seiner vorgegebenen Kriterien.

Ausschreibungsportale bieten zusätzliche Möglichkeiten an, damit potenzielle Auftraggeber und Auftragnehmer sich informieren und in Kontakt treten können, z. B. einen Informationsdienst, z. B. Auftraggeber- /-nehmerkontakte, „Investitionsvorhaben“ (dtad), CRM- und Workflow-Funktionen (z. B. www.dtad.com, dtpv.de, www.infodienst-ausschreibungen.de, www.it-ausschreibung.de, www.evergabe.de, www.vergabe.rib.de, <https://vergabe.fraunhofer.de>, Glossar in www.dtad.com/de/glossar).

Vorteile der elektronischen Vergabe

- Die Ausschreibungsdatenbank ist i.d.R. tagesaktuell gepflegt.
- Potenzielle Auftragnehmer können ihre Suche/Selektion regional und nach anderen Kriterien einschränken bzw. passgenau ausrichten.
- Die Mitarbeiter der Plattform bieten professionelle Unterstützungsdienstleistungen.
- Der Informationsaustausch zwischen Auftraggeber und Bieter kann vollständig elektronisch abgewickelt werden.
- Die Angebotsbearbeitung und -abgabe ist rund um die Uhr und vielerorts möglich.
- Die Vergabevorgänge werden vereinfacht, standardisiert, rechtssicherer und nachvollziehbar.
- Leistungsverzeichnisse und weitere Anlagen können einfach ergänzt und aktualisiert werden.
- Formale Fehler können durch Plausibilitätsprüfungen vermieden werden.
- Kosten für Vervielfältigung und Versand von Vergabeunterlagen entfallen.
- Auftragnehmer können über Erfassungsmasken strukturiert ihre Angebote erfassen, was für die Auftragnehmer die Erstellung der Arbeit und für den Auftraggeber Angebotsprüfung und -vergleich erleichtert.
- Ein Vergabemanager erleichtert die Vorgangsbearbeitung und die Angebotsauswahl.
- Über eine digitale Signatur können Angebote rechtssicher unterzeichnet werden.

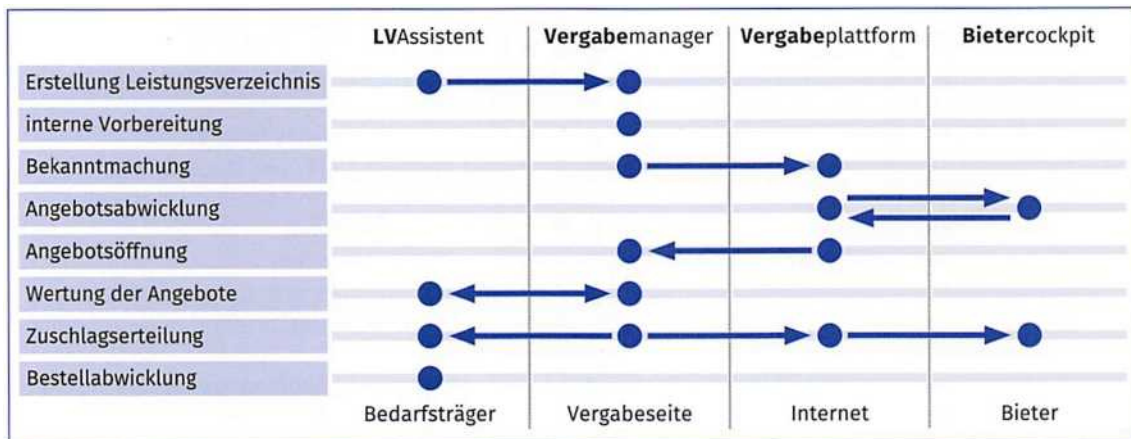
Auftraggeber müssen ihren potenziellen Auftragnehmern alle Informationen geben, die zur Abgabe von Angeboten notwendig sind bzw. bei öffentlichen Auftraggebern gesetzlich gefordert werden. Bevor funktionale und nicht funktionale Eigenschaften beschrieben werden, müssen übergreifende bzw. allgemeinere Angaben erstellt werden, damit potenzielle Auftragnehmer die Ausschreibung oder Aufforderung zur Angebotsabgabe finden können. Ausschreibungsportale sehen dazu z. B. eine Titelangabe und eine Kurzerläuterung vor. Bei Servern ist zu klären, ob nur ein Server, welche Serverart (z.B. VDI-, SDD-, Terminal-, Back-up-Server) und welche Zusatzpositionen zu beschaffen sind. Die Kurzbeschreibung sollte angeben, wofür der Servereinsatz vorgesehen ist, und der Umfang der Beschaffungsmaßnahme beschrieben werden.

Ausschreibungskomponenten

- Bekanntmachung, Titel, Auftragsgegenstand, Kurzerläuterung, Angebotsformular
- Unterteilung in Lose, Teillöse, d. h. Angebotsteile, die separat vergeben werden können
- Leistungsbeschreibungen (Pflichtangaben, optionale Angaben, Wertungsschema für den qualitativen Angebotsvergleich mit Kriterien und Prozentanteilen)
- Anlagen (z.B. Grundpläne, Datei Leistungsbeschreibung, Nebenangebote, Angebotsunterlagen, Preisblatt, Fragebogen zur Eignungsprüfung)
- Vergabeunterlagen im Liefer- und Dienstleistungsverfahren
- Rechtliche Aspekte (Teilnehmerantrag, Rechtsvorgaben, Angebotsrückzug, Vergabeverfahren, Unterschrift, digitale Signatur)

Anhand des folgenden Vergabeprozesses können die einzelnen Prozessschritte nach der Erfassung der Grunddaten einer Vergabeart bzw. ab der Leistungsbeschreibung bis hin zur Bestellabwicklung unterschieden werden. Für einen geregelten und transparenten Vergabeprozess ist es sehr wichtig, vorgegebene Abläufe auch einzuhalten. Die Vergabemodule sind bezogen auf die Prozessbeteiligten entwickelt worden und lassen die Schnittstellen der Module erkennen. Erfolgen die Ausschreibungen nach VOL (A) (Dienst- oder Lieferleistungen), ist die Zuschlagsvergabe nicht öffentlich. Bieter können aber bereits bei der Angebotsabgabe darum bitten, im Fall der Ablehnung des Angebots über die Gründe informiert zu werden. Wichtig ist die Einhaltung aller vorgegebenen Termine. Wenn Termine verpasst werden, kann man ohne eine Ausnahmegestattung nicht mehr teilnehmen.

Beispiel: Vergabeprozess über den Vergabemanager in evergabe.de



Die folgenden Kalkulationsblätter wurden vom Auftraggeber erstellt, um den Anbietern eine Vorlage zu bieten, die im Angebotsvergleich gut weiterverwendet werden kann. Diese werden i.d.R. als Anlagen den Auftragnehmern zur Verfügung gestellt und in Ausschreibungsportalen hochgeladen. Portale bieten aber auch die Möglichkeit, in Erfassungsmasken alle Positionen mit den entsprechenden Leistungsangaben detailliert zu erfassen und Ergänzungen der Auftragnehmer zu den gebotenen Leistungen, Preisen und Rabatten vorzunehmen.

A	B	C	D	E	F	G
1	Stadt Nettesheim					
2	Ausschreibung Schuldigitalisierung: Server, Software, Unterstützung					
3	Anlage 2 der Leistungsbeschreibung	Hinweise				
4	Preisblatt	Nur grün hinterlegte Felder ausfüllen!				
5						
Teillos Nr.	Bezeichnung Teillöse von Los 1	Menge	Hersteller Artikel Nr.	Detaillierte Produkt-/Leistungsbezeichnung/Leistungsbeschreibung	Kaufpreis/Einheit	Gesamtpreis
7	1 Server komplett	1				0,00 €
8	2 Rack komplett	1				0,00 €
9	3 Microsoft Windows Server 2022 Standard 24 Core	1				0,00 €
10	4 vmware vSphere 7 Enterprise plus inkl Subscription 24 Monate	1				0,00 €
11	5 NAS komplett	1				0,00 €
12	6 USV komplett	1				0,00 €
13	7 Firewall komplett	1				0,00 €
14	8 AntiVirus und Internet Security Lösung komplett	1				0,00 €
15	9 Installation pauschal	1				0,00 €
16	10 Datenübernahme pauschal	1				0,00 €
17					Summe:	0,00 €
18						
Teillos Nr.	Bezeichnung Teillöse von Los 2	Menge	Hersteller Artikel Nr.	Detaillierte Produkt-/Leistungsbezeichnung/Leistungsbeschreibung	Kosten pauschal	Gesamtpreis
20	1 Pädagogische Netzwerkmanagementlösung, Laufzeit 24 Monate	1				0,00 €
21	2 Internetfilter	122				0,00 €
22	3 Installation komplett und Schulung pauschal	1				0,00 €
23					Summe:	0,00 €
24						
Teillos Nr.	Bezeichnung Teillöse von LOS 3	Menge	Hersteller Artikel Nr.	Detaillierte Produkt-/Leistungsbezeichnung/Leistungsbeschreibung	Mietpreis / Jahr	Gesamtpreis
26	1 Mobile Device Management für Apple iPads, Laufzeit 24 Monate	600				0,00 €
27						
28					Gesamt netto:	0,00 €
29					Gewährter Rabatt (in Euro):	0,00 €
30					Gesamt netto abzgl. Rabatt (in Euro):	0,00 €
31					zzgl. 19 % Mehrwertsteuer (USt.):	0,00 €
32	Hinweis: Gelb hinterlegter Betrag muss mit VHB-Formblatt 633 übereinstimmen!					Gesamtsumme brutto: 0,00 €

Da die Anzahl der Arbeitsstunden noch nicht genau eingeschätzt werden kann, werden die Stundensätze abgefragt und in den Angebotsvergleich einbezogen.

A	B	C	D
1	Stadt Nettesheim		
2	Ausschreibung Schuldigitalisierung: Server, Software, Unterstützung		
3	Anlage 2 der Leistungsbeschreibung	Hinweise	
4	Preisblatt Stundensätze	Nur grün hinterlegte Felder ausfüllen!	
5			
Teillos Nr.	Bezeichnung Teillöse von Los 4	Menge	Stundensatz netto
7	1 Techniker	1	
8	2 System Engineer	1	
9	3 Auszubildender	1	

LE 2 - Funktionale Anforderungen planen

Mithilfe des Lastenheftes wird aus den funktionalen Anforderungen des Kunden ein Lösungsvorschlag erarbeitet. Dieses Kapitel beschreibt, was bei der Planung berücksichtigt und dokumentiert werden sollte.

LE 3 - Netzwerk

Wenn für einen Kunden ein Netzwerk eingerichtet werden soll, so fallen darunter neben dem WAN-Anschluss und dem physikalischen Netzwerk oft auch WLAN, VLAN, VPN und ggf. PoE.

Glasfaseranschluss planen

Bei der Planung eines Glasfaseranschlusses ist Folgendes zu berücksichtigen:

Glasfaseranschluss	
FTTB	Der Kunde erhält einen Glasfaseranschluss im Gebäude „Fibre to the Building“. Von dort werden die einzelnen Wohnungen über Kupferkabel angeschlossen.
FTTC	Der Glasfaseranschluss wird bis zum Straßenverteilerkasten/Kabelverzweiger verlegt, „Fibre to the curb“ (Straßenrand). Von dort aus werden die bereits vorhandenen Kupferkabel genutzt.
FTTD	Der Kunde erhält bei „Fibre to the desk“ einen Glasfaseranschluss bis zu seiner Anschlussdose.
FTTH	Der Kunde erhält einen Glasfaseranschluss im Gebäude „Fibre to the home“. Von dort werden die vorhandenen Kupferkabel genutzt.
Zwangstrennung	Auch bei Glasfaser ist es üblich, dass der Provider die Internetverbindung beispielsweise einmal pro Woche aus technischen Gründen trennt und wiederherstellt.
Fest/ dynamische IP-Adresse	Wie auch bei den DSL-Produkten (Kupferkabel) erhält der Kunde eine dynamische IP-Adresse, oft eine nicht öffentliche IPv4-Adresse und eine öffentliche IPv6-Adresse. Für IPv4 erfolgt die Adressumsetzung über ein NAT Gateway des Providers.

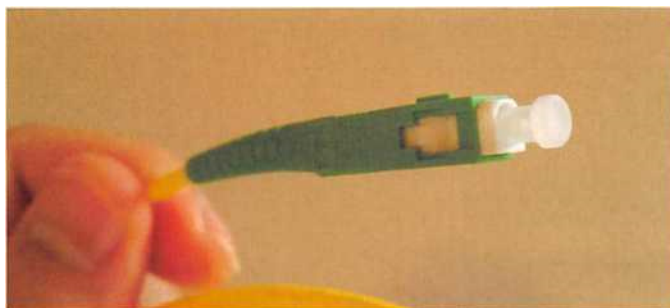
NDB 100 <i>Business</i> Feste IP	NDB 250 <i>Business</i> Feste IP	NDB 500 <i>Business</i> Feste IP	NDB 1000 <i>Business</i> Feste IP
100 Mbit/s Download	250 Mbit/s Download	500 Mbit/s Download	1000 Mbit/s Download
100 Mbit/s Upload	250 Mbit/s Upload	500 Mbit/s Upload	1000 Mbit/s Upload
199,00 € mtl.	299,00 € mtl.	499,00 € mtl.	Preis auf Anfrage

Nach der Ermittlung des Glasfaseranbieters für das Gebäude des Kunden kann der Kunde zwischen verschiedenen Tarifen wählen. Geschäftskunden nutzen häufig sogenannte symmetrische Anschlüsse („Business Tarife“). Dabei entspricht die Datenübertragungsrate des Uploads der des Downloads.

Beispielangebot für Glasfaseranschlüsse für Geschäftskunden



Glasfaseranschluss im Hausübergabepunkt mit Lichtwellenleiter



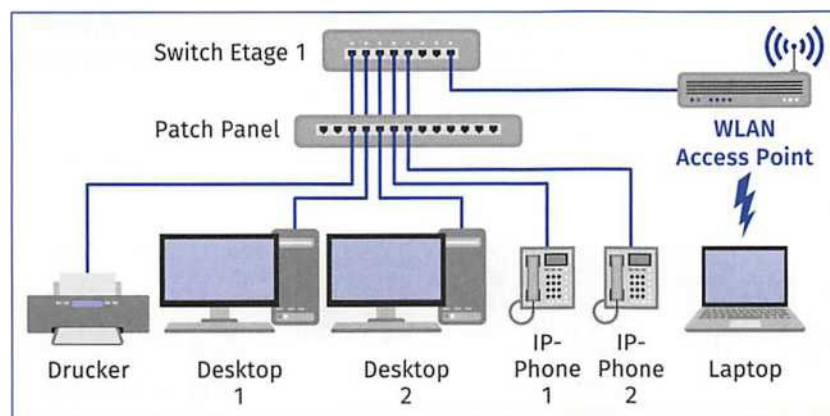
LC-Stecker des Lichtwellenleiters (LC = Lucent Connector)

Netzwerk planen

Bei der Planung eines Netzwerkes wird die Vernetzung von Gebäuden (siehe Glasfaseranschluss planen), die Vernetzung zwischen den Etagen und die Vernetzung innerhalb der Etagen unterschieden. Dabei können, je nach Bedarf des Kunden, Glasfaser, Twisted Pair, WLAN und, wenn keine Leitung verlegt werden darf, Powerline zum Einsatz kommen. Bestimmende Größen sind immer Datendurchsatzraten und Kosten.

Vernetzung innerhalb einer Etage planen

Bei der Vernetzung innerhalb einer Etage (siehe Abbildung unten) werden z. B. Cat6-Leitungen von den Netzwerkdosen zum Patch Panel geplant und die Leitungslängen notiert. Patch Panel und Switch befinden sich in unmittelbarer Nähe zueinander, z.B. in einem 19-Zoll-Rack. Kurze Patch-Kabel verbinden die RJ45-Ports von Switch und Patch Panel. Die Anzahl Ports von Switch und Patch Panel (8, 16, 24 oder 48) werden entsprechend dem Kundenwunsch (Anzahl Netzwerkdosen im Raum) dimensioniert. Werden mehr Ports benötigt, so werden die Switches kaskadiert.



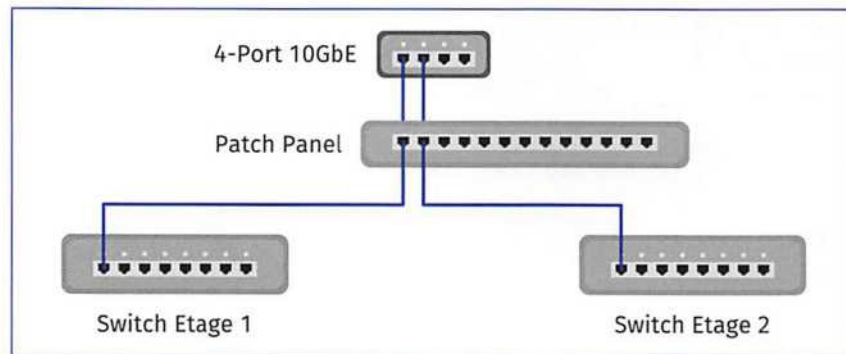
Netzwerkstage

Vernetzung innerhalb des Gebäudes planen

Bei der Vernetzung innerhalb des Gebäudes werden die Leitungen von den Switches der Etagen (Access Switches) zum Gebäude- bzw. Hauptanschlussraum geplant. Die Leitungen laufen in diesem Raum in einem Patch Panel zusammen.

Patch Panel und Switch (in der Abbildung der 4-Port) befinden sich in unmittelbarer Nähe zueinander, z.B. in einem 19-Zoll-Rack. Kurze Patchkabel verbinden die RJ45-Ports von Switch und Patch Panel.

Die folgende Grafik zeigt schematisch die Verkabelung innerhalb eines Gebäudes.



Vernetzung innerhalb des Gebäudes

Bei der Planung logischer Netzwerke muss ggf. eine DMZ geplant werden.

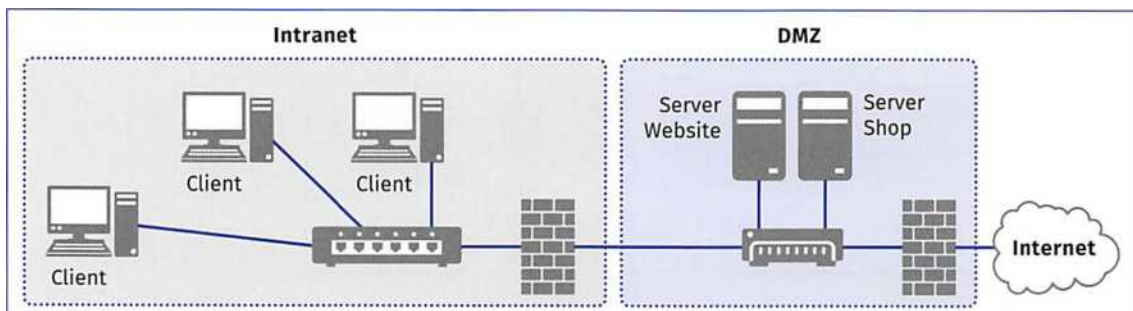
Demilitarized Zone (DMZ)

Bei einer Demilitarized Zone (DMZ) handelt es sich um eine sogenannte „entmilitarisierte“ Zone des lokalen Netzwerks. Alle Server, die sich im Firmennetz befinden und aus dem Internet erreichbar sind, sind auch angreifbar. Aus diesem Grund ist das Intranet selbst mit mindestens einer weiteren Firewall von diesen Servern abgeschirmt. Ein Extranet wiederum enthält die Server, die nur von bestimmten Personen aus dem Internet heraus aufrufbar sein sollen, z.B. Kooperationspartner oder Lieferanten.

Beispiel:

Das Bild zeigt vereinfacht, dass sich die DMZ zwischen zwei Firewalls befindet. Darin werden Server wie die eigene Webseite, das Shop-System etc. platziert.

Gegenentwurf: Zur Minimierung des Angriffsvektors auf ein Firmennetz können alternativ oder zusätzlich auch folgende Maßnahmen ergriffen werden: Software defined Networks (wenn die Dienste im Firmennetz verbleiben sollen) und das Auslagern von Diensten in die Cloud (Zero Trust Strategie).



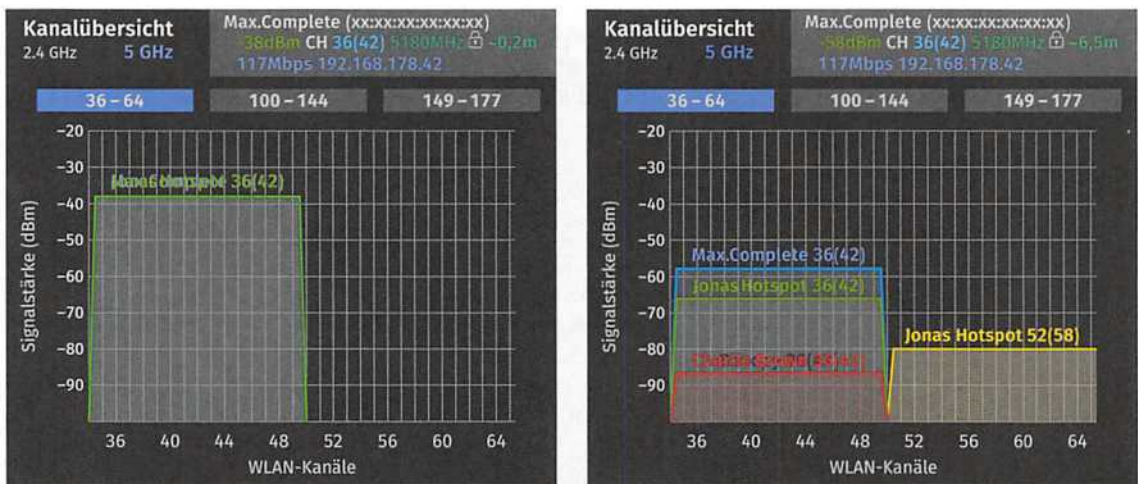
Mit der Planung des Netzwerkes müssen ebenfalls die IP-Adressierungsschemata festgelegt werden. Sollen IPv4-Adressen und/oder IPv6-Adressen genutzt werden? Für alle Subnetze gemäß der o.a. Verkabelung und der WLAN, VLAN bzw. VPN müssen IP-Adressen festgelegt werden.

IP-Adressierungsschema planen (gilt für alle Netzwerke WLAN, VLAN, VPN etc.)																																	
Netzmaske IPv4	Die Netzmaske bzw. Subnetzmaske legt fest, welche IP-Adressen eine Netzwerkkomponente erreichen kann. Bei 24 gesetzten Bits ist die Subnetzmaske 255.255.255.0. Bei solch einem 24er-Netz - kurze Schreibweise /24 - verbleiben 8 Bit, also 256 Adressen für die Vergabe. Die kleinste und größte Adresse sind stets reserviert. Die kleinste Adresse, die Netzwerk-Adresse, adressiert das Netz selbst. Die größte Adresse ist für Broadcasts reserviert: Ein /32er-Netz ist nicht nutzbar, $2^0 - 2$ ist negativ. Ein /31er-Netz erlaubt keine Vergabe von Adressen, $2^1 - 2 = 0$ Ein /30er-Netz erlaubt die Vergabe von 2 Adressen, $2^2 - 2 = 2$ Ein /29er-Netz erlaubt die Vergabe von 6 Adressen, $2^3 - 2 = 6$ Ein /28er-Netz erlaubt die Vergabe von 14 Adressen, $2^4 - 2 = 14$ usw.																																
IPv4- Adressen	<i>Beispiel 1:</i> Bei einer IP-Adresse 192.168.178.52/24 ist der Netzwerkteil 192.168.178. Die erste nutzbare IP-Adresse ist 192.168.178.1 und die letzte 192.168.178.254. <table> <tr><td>Hostaddress</td><td>- 192.168.178.52</td></tr> <tr><td>Networkaddress</td><td>- 192.168.178.0</td></tr> <tr><td>Network mask</td><td>- 255.255.255.0</td></tr> <tr><td>Network mask (bits)</td><td>- 24</td></tr> <tr><td>Broadcastaddress</td><td>- 192.168.178.255</td></tr> </table> (IP Broadcasts kommen bei DHCP- und BOOTP-Clients zum Einsatz um den entsprechenden Server (DHCP/BOOTP) zu finden. Die Anfrage geht an alle Netzwerkkomponenten in dieser Domäne.) <table> <tr><td>Adressen insgesamt</td><td>- 256</td></tr> <tr><td>Network range</td><td>- 192.168.178.0 - 192.168.178.255</td></tr> <tr><td>Usable range</td><td>- 192.168.178.1 - 192.168.178.254</td></tr> </table> <i>Beispiel 2:</i> IP-Adresse 192.168.178.52/27 <table> <tr><td>Hostaddress</td><td>- 192.168.178.52</td></tr> <tr><td>Network address</td><td>- 192.168.178.32</td></tr> <tr><td>Network mask</td><td>- 255.255.255.224</td></tr> <tr><td>Network mask (bits)</td><td>- 27</td></tr> <tr><td>Broadcast address</td><td>- 192.168.178.63</td></tr> <tr><td>Addresses in network</td><td>- 32</td></tr> <tr><td>Network range</td><td>- 192.168.178.32 - 192.168.178.63</td></tr> <tr><td>Usable range</td><td>- 192.168.178.33 - 192.168.178.62</td></tr> </table>	Hostaddress	- 192.168.178.52	Networkaddress	- 192.168.178.0	Network mask	- 255.255.255.0	Network mask (bits)	- 24	Broadcastaddress	- 192.168.178.255	Adressen insgesamt	- 256	Network range	- 192.168.178.0 - 192.168.178.255	Usable range	- 192.168.178.1 - 192.168.178.254	Hostaddress	- 192.168.178.52	Network address	- 192.168.178.32	Network mask	- 255.255.255.224	Network mask (bits)	- 27	Broadcast address	- 192.168.178.63	Addresses in network	- 32	Network range	- 192.168.178.32 - 192.168.178.63	Usable range	- 192.168.178.33 - 192.168.178.62
Hostaddress	- 192.168.178.52																																
Networkaddress	- 192.168.178.0																																
Network mask	- 255.255.255.0																																
Network mask (bits)	- 24																																
Broadcastaddress	- 192.168.178.255																																
Adressen insgesamt	- 256																																
Network range	- 192.168.178.0 - 192.168.178.255																																
Usable range	- 192.168.178.1 - 192.168.178.254																																
Hostaddress	- 192.168.178.52																																
Network address	- 192.168.178.32																																
Network mask	- 255.255.255.224																																
Network mask (bits)	- 27																																
Broadcast address	- 192.168.178.63																																
Addresses in network	- 32																																
Network range	- 192.168.178.32 - 192.168.178.63																																
Usable range	- 192.168.178.33 - 192.168.178.62																																
Netzmaske IPv6	IPv6-Adressen haben eine Länge von 128 Bits. Die Angabe von /64 bedeutet, dass der Netzwerk-Teil 64 Bits lang ist, der Interface Identifier (Geräteanteil) ebenfalls 64 Bits.																																
IPv6- Adressen	<i>Beispiel 1:</i> Bei einer IP-Adresse 2a01:c207:3005:3137::1/64 ist der Netzwerkanteil 2a01:c207:3005:3137, der Interface Identifier ist die 0000:0000:0000:0001 <table> <tr><td>Expanded Address</td><td>- 2a01:c207:3005:3137:0000:0000:0000:0001</td></tr> <tr><td>Compressed address</td><td>- 2a01:c207:3005:3137::1</td></tr> <tr><td>Subnet prefix (masked)</td><td>- 2a01:c207:3005:3137:0:0:0:0/64</td></tr> <tr><td>Address ID (masked)</td><td>- 0:0:0:0:0:0:1 /64</td></tr> <tr><td>Prefixaddress</td><td>- ffff:ffff:ffff:ffff:0:0:0:0</td></tr> <tr><td>Prefix length</td><td>- 64</td></tr> <tr><td>Network range</td><td>- 2a01:c207:3005:3137:0000:0000:0000:0000 - 2a01:c207:3005:3137:ffff:ffff:ffff:ffff</td></tr> </table>	Expanded Address	- 2a01:c207:3005:3137:0000:0000:0000:0001	Compressed address	- 2a01:c207:3005:3137::1	Subnet prefix (masked)	- 2a01:c207:3005:3137:0:0:0:0/64	Address ID (masked)	- 0:0:0:0:0:0:1 /64	Prefixaddress	- ffff:ffff:ffff:ffff:0:0:0:0	Prefix length	- 64	Network range	- 2a01:c207:3005:3137:0000:0000:0000:0000 - 2a01:c207:3005:3137:ffff:ffff:ffff:ffff																		
Expanded Address	- 2a01:c207:3005:3137:0000:0000:0000:0001																																
Compressed address	- 2a01:c207:3005:3137::1																																
Subnet prefix (masked)	- 2a01:c207:3005:3137:0:0:0:0/64																																
Address ID (masked)	- 0:0:0:0:0:0:1 /64																																
Prefixaddress	- ffff:ffff:ffff:ffff:0:0:0:0																																
Prefix length	- 64																																
Network range	- 2a01:c207:3005:3137:0000:0000:0000:0000 - 2a01:c207:3005:3137:ffff:ffff:ffff:ffff																																

IP-Adressierungsschema planen (gilt für alle Netzwerke WLAN, VLAN, VPN etc.)	
IPv6-Adressen	<i>Beispiel 2:</i> IP-Adresse 2a01:c207:3005:3137::1 /59 Expanded Address - 2a01:c207:3005:3137:0000:0000:0000:0001 Compressed address - 2a01:c207:3005:3137::1 Subnet prefix (masked) - 2a01:c207:3005:3120:0:0:0:0/59 Address ID (masked) - 0:0:0:17:0:0:0:1 /59 Prefixaddress - ffff:ffff:ffff:ffe:0:0:0:0 Prefix length - 59 Network range - 2a01:c207:3005:3120:0000:0000:0000:0000 - 2a01:c207:3005:313f:ffff:ffff:ffff:ffff

WLAN planen

Der Kunde erhält einen oder mehrere WLAN-Access-Points, um sein Gebäude optimal „auszuleuchten“. Über eine Vorab-Diagnose, z.B. mit einem WLAN-Scanner wie dem „WiFi-Analyzer“ (<https://github.com/VREMSoftwareDevelopment/WiFiAnalyzer>), wurde in der Ist-Analyse ermittelt, wie stark das WLAN-Signal in den bereits vorhandenen Räumen ist.



Signalstärke für das 5 GHz und 2,4 GHz Netz im Raum 1 (links) und in Raum 2 (rechts).

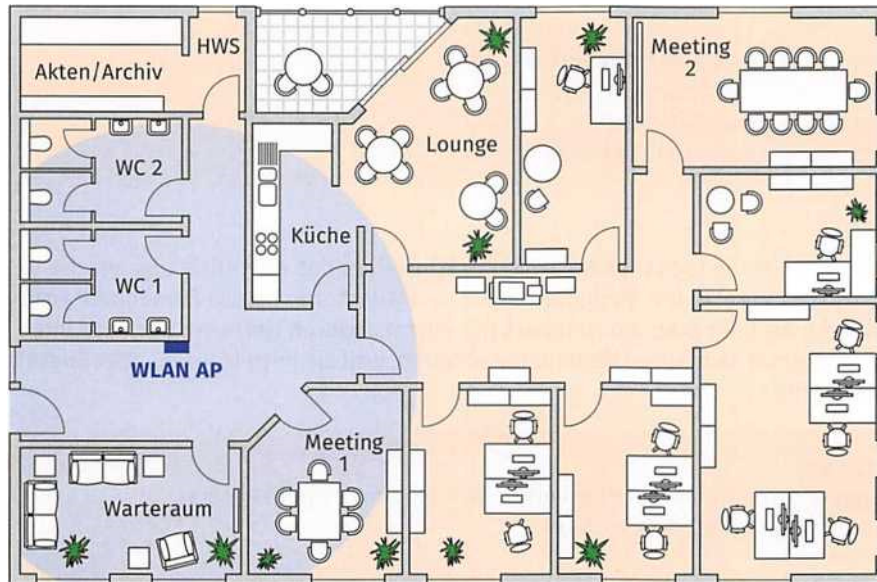
Signalstärke

Die Signalstärke wird logarithmisch in dBm (Dezibel Milliwatt) angegeben. Für die Sendeleistung sind es positive Werte, für die Empfangsleistung negative Werte.

WLAN-Signalstärke	
-0 dBm	Dies ist der höchste und zugleich beste Wert für das Empfangen. Er entspricht einem Milliwatt (mW) Leistung.
-10 dBm	Dieser Wert entspricht einer Leistung von 0,1 mW.
-20 dBm	Dieser Wert entspricht einer Leistung von 0,01 mW.
-30 dBm	Dieser Wert entspricht einer Leistung von 0,001 mW.
-30 dBm bis -40 dBm	Werte in diesem Bereich entsprechen einer guten Signalstärke.
-85 dBm	Werte unterhalb von -85 dBm sind als kritisch zu betrachten. Eine stabile Verbindung kann nicht aufgebaut werden.

Mit den Ergebnissen der durchgeführten Messungen werden die Anzahl und Platzierung der Access Points geplant und im Pflichtenheft mittels eines Raumplans (siehe folgende Abbildung) dokumentiert.

Access Points sollten nach Möglichkeit in die Nähe bereits vorhandener Netzwerkdo- sen platziert werden. Ist bereits ein Access Point vorhanden, so können weitere Access Points als Repeater konfiguriert werden - sie benötigen dann keine Netzwerkdo- se.



WLAN ist bereits im Warteraum, Meetingraum 1 und im WC vorhanden.

Im Pflichtenheft wird dokumentiert, wie viele Access Points platziert werden sollen und wo. Im obigen Beispiel wird ein Access Point platziert, um den Warteraum, Meetingraum 1 und das WC mit einem Gast- WLAN auszustatten.

VLAN planen

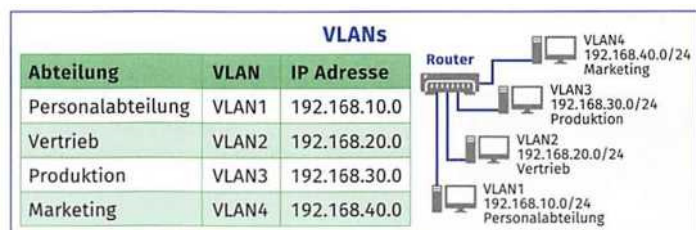
Virtuelle Local Area Networks (VLAN), erlauben das Festlegen logischer Netzwerke in einem LAN. Mit der Einrichtung von virtuellen LANs können Zugriffe gezielt geregelt werden. Voraussetzung dafür ist, dass bei einem physikalischen Netz die entsprechenden Netzwerkkomponenten, z. B. Switches, VLAN-fähig sind. (Dies hängt von der Netzwerkplanung ab.)

Der Standard IEEE802.1Q unterstützt paketbasierte „getaggte“ VLANs. Jedes Netzwerkpaket enthält einen Tag, die sogenannte VLAN-IDs. Das Netzwerk lässt sich über diese VLAN-IDs segmentieren, wodurch die Netzwerkperformance gesteigert wird.

Beispiel:

Bei den Netzwerkkomponenten findet sich die VLAN-Konfiguration im Menü „Port Management“.

Jedem Port wird per Konfiguration eine VLAN-ID zugewiesen und zudem, ob ein Inter-VLAN-Routing für diesen Port erlaubt ist.



VLANs definieren logische Netzwerke auf OSI Layer 2.

VLANs finden Anwendung bei: VoIP-Gesprächen, https-Traffic oder der Live-Migration einer virtuellen Maschine von einem physikalischen Server auf einen anderen - all diese Verbindungen erzeugen unterschiedlich viel Datenverkehr. Mittels VLAN kann dieser Traffic gezielt zwischen

den entsprechenden Kommunikationspartnern geleitet werden, ohne dass die anderen Kommunikationspartner, welche sich im gleichen physikalischen LAN befinden, beeinträchtigt werden.

VLANs ermöglichen

- die logische Gruppierung von Netzwerkkomponenten,
- eine Optimierung des Netzwerkverkehrs,
- damit eine Erhöhung der Netzwerksicherheit,
- ebenfalls eine Priorisierung von Netzwerkpaketen.

VPN planen

Ein Virtual Private Network (VPN) ist ein logisches Netzwerk, welches über das öffentlich zugängliche Internet abgebildet wird. Es wird eingesetzt, um Niederlassungen und Mitarbeiter an das Firmennetz anzubinden. Bei einem VPN wird ein Rechner oder ein Netzwerk mit einem anderen Netzwerk über das Internet verbunden. Niemand im Internet kann diese Verbindung abhören, weil sie mittels IPsec, "WireGuard", "OpenVPN" o.Ä. verschlüsselt wird.

VPNs werden eingesetzt, um

- a) Heimarbeitsplätze der Mitarbeiter an das Firmennetz anzubinden (Remote Access),
- b) Filialen an die Zentrale anzubinden (Site-to-Site),
- c) IoT-Geräte anzubinden.

Technisch betrachtet hält die Zentrale dafür sogenannte VPN-Zugänge vor. Dieses kann eine Software sein, z.B. „OpenVPN“ (<https://openvpn.net>) oder aber ein Router mit VPN-Funktionalität, ein sogenannter VPN-Router. Auf der Gegenseite wird im Fall a) und c) oft ein VPN-Client genutzt, im Fall b) allerdings ein VPN-Router. Ist der VPN Tunnel etabliert, so hat der Client eine firmeninterne IP-Adresse zugewiesen bekommen. Sämtliche Verbindungen des Clients, der Filiale bzw. des IoT-Gerätes werden nun über diesen Tunnel geleitet.

VPNs können technisch gesehen einen Flaschenhals darstellen, z.B. wenn mehrere VPN-Verbindungen gleichzeitig gehalten werden müssen und Mitarbeiter darüber Videokonferenzen durchführen. Der VPN-Router muss entsprechend performant gewählt werden.



Beispiel für eine VPN-Client-Software: Linux Netzwerkverwaltung

IPsec, die Internet Protocol Security, arbeitet auf dem OSI Layer 3, der Vermittlungsschicht. Das Protokoll bietet Vertraulichkeit, Integrität und Schutz vor Manipulation durch Verschlüsselung und Authentifizierung. IPsec ist in der RFC4301 dokumentiert (<https://tools.ietf.org/html/rfc4301>).

Die Herausforderung beim Aufbau von sicheren Leitungen über das öffentlich zugängliche Internet ist, dass der Aufbau selbst abgehört werden kann. Wie kann nun ein gemeinsamer zu nutzender Schlüssel (Shared Key, symmetrischer Schlüssel) ausgetauscht werden, ohne dass der Rest der Welt diesen mitlesen kann? Dieses wird, wie es auch bei „TLS“, „AES“ und „openssh“ eingesetzt wird, über das Diffie-Hellman-Protokoll erreicht. Dabei tauschen die zwei Kommunikationspartner ihre öffentlichen Schlüssel über das Internet aus (public/private Key Verfahren). Nun kann der öffentliche Schlüssel des anderen zum Verschlüsseln der zu sendenden Nachricht genutzt werden. Da nur der Empfänger den privaten Schlüssel hat, kann auch nur dieser die Nachricht entschlüsseln.

PoE planen

Power over Ethernet (PoE) ermöglicht die Nutzung von Cat5/5e/6-Netzkabeln für die Stromversorgung von Netzwerkkomponenten. So können Endgeräte, z.B. IP-Telefone, IP-Kameras, Wireless Access Points (Powered Devices), ohne separate Stromversorgung über das Netzkabel betrieben werden. PoE ist in der IEEE 802.3af dokumentiert. Ohne Verlegung von elektrischen Leitungen können so Peripheriegeräte in Betrieb genommen werden.

Es ist stets zu berücksichtigen, welchen Leistungsbedarf die Powered Devices haben, wie viel Leistung der Switch, z.B. PoE-Switch, pro Port liefert und mit welcher Leitungserwärmung zu rechnen ist:

- PoE nach IEEE 802.af liefert netto bis zu 12,95 W.
- PoE+ nach IEEE 802.at liefert bis zu 25 W.
- PoE++ nach IEEE 802.bt liefert bis zu 65 W.



Um PoE nutzen zu können, wird ein Energieversorger (Power Sourcing Equipment) benötigt, also ein PoE-fähiger Switch (End-Span) oder aber PoE-Injektoren (Mid-Span), z. B. in Form von Power-Hubs oder PoE-Adapter. Über eine zentrale unterbrechungsfreie Stromversorgung (USV) können PoE-Geräte abgesichert werden.

LE 4 - Netzwerkkomponenten planen

WLAN-Access-Points planen

WLAN-Access-Points ermöglichen den Anwendern den Zugriff auf das lokale Netzwerk und stellen somit eine sicherheitskritische Komponente dar.

Bei der Planung von WLAN-Access-Points ist Folgendes zu berücksichtigen:

- Sollen Gastnetze eingerichtet werden und falls ja, sollen/müssen diese in das Firmennetz integriert werden?
Da Access Points bei entsprechender Planung über das Internet erreichbar sein können, lassen sie sich auch über das Internet konfigurieren. Einige Hersteller bieten ein Internetportal (Management Cloud) an, über welche sich alle Switches mit Gastnetz zentral konfigurieren lassen.
- Sollen alle Access Points ein gemeinsames Mesh-Netz aufspannen oder jeder Access Point ein separates Netz?
Der aktuelle Sicherheitsstandard WPA3 wird nur von neueren Endgeräten unterstützt (Stand: 2021). Access Points sollten daher auf Wunsch des Kunden die WPA2- und parallel die WPA3- Verschlüsselung unterstützen. So wird gewährleistet, dass auch ältere Geräte wie ältere Smartphones Zugriff erhalten.

WLAN-Absicherung	
Eigenschaft	Beschreibung
SSID	Name des WLAN-Netzes
WPA3	Standard-Verschlüsselungsverfahren für WLAN-Netze; es unterstützt Perfect Forward Secrecy. Dabei werden die Sitzungsschlüssel immer neu erstellt und niemals von einem Master Key abgeleitet: Ein nachträgliches Errechnen von Session Keys ist somit, trotz möglicher Kenntnis des Master Keys, nicht möglich.
Eigenschaft	Beschreibung

WPA2 (veraltet)	WPA2 nutzt den Advanced Encryption Standard (AES) für das Verschlüsseln von WLAN-Netzen. Aufgrund von Schwachstellen sollte allerdings WPA3 genutzt werden.
WPA (veraltet)	WiFi Protected Access ist der Nachfolger von WEP und ebenfalls ein veraltetes Verschlüsselungsverfahren, welches wegen mangelnder Sicherheit nicht mehr genutzt werden sollte.
WEP (veraltet)	Verschlüsselungsverfahren für WLAN-Netze, welches aufgrund mangelnder Sicherheit nicht mehr genutzt werden sollte.
WLAN-Schlüssel	Der Netzwerkschlüssel bzw. das Passwort für das WLAN wird vom Administrator des Kunden vergeben. Es sollte eine Zeichenlänge von mindestens 20 besitzen.
WPS	Über das WiFi Protected Setup lassen sich neue Geräte einfacher im WLAN aufnehmen, z. B. durch Tastendruck am Access Point (abhängig vom Access Point).
Mesh	Mit der Mesh-Funktion können mehrere WLAN-Access-Points ein gemeinsames WLAN aufspannen. Die entsprechenden Geräte verbinden sich immer mit dem Access Point in nächster Nähe bzw. mit der größten Signalstärke.

Switches planen

Switches werden je nach Einsatzgebiet als **Core Switch** (für Hochgeschwindigkeitsnetze), **Distribution Switch** (Gebäudeverteiler) oder **Access Switch** (Anschluss der Endgeräte) bezeichnet. Zur Vermeidung sogenannter Broadcast-Stürme sind diese über das Spanning Tree Protocol (STP) verbunden. Switches mit dem Nachfolger RSTP (IEEE 802.1w, Rapid Reconfiguration of Spanning Tree, <https://www.ieee802.org/1/pages/802.1w.html>) sind in großen Netzen zu bevorzugen.

Spanning Tree Protocol (STP) und Rapid Spanning Tree Protocol (RSTP)

Das Spanning Tree Protocol (STP) sowie die Weiterentwicklung, das Rapid Spanning Tree Protocol (RSTP), dienen dazu, „kreisende“ Netzwerkpakete in LANs zu identifizieren und zu deaktivieren. Diese entstehen, wenn Switches (auch MAC-Bridges genannt) so konfiguriert werden, dass es parallele Wege gibt.

STP-/RSTP-fähige Switches bauen einen Verbindungsbaum auf. Werden parallele Verbindungen identifiziert, so werden sie deaktiviert. Bei Ausfall der Hauptverbindung wird die parallele Verbindung wieder aktiviert. Dabei kommunizieren die Switches untereinander über Bridge Protocol Data Units. Sie senden sich gegenseitig ihre Konfigurationen zu. Tritt eine Änderung auf, wird diese ebenfalls per Multicast den anderen Switches mitgeteilt.

Typische Switches (Layer-2-Switches) entscheiden aufgrund der MAC-Adressen, an welchen Port ein eingetroffenes Paket weitergeleitet wird. Layer-3-Switches hingegen können diese Entscheidung aufgrund der IP-Adresse treffen und übernehmen somit die Aufgabe eines Routers. Diese Switches können, wie auch Router, jedem Port ein bestimmtes Subnetz zuweisen.

Firewall planen

Bei der Planung der Firewall ist darauf zu achten,

- welche Art Firewall eingesetzt werden soll: Paketfilter, Inhaltsfilter, Intrusion Detection und Prevention, etc.,
- welche Performance die Firewall liefern soll, damit sie nicht als „Flaschenhals“ verkommt,
- ob die Firewall Virtualisiert betrieben werden darf,
- welchen Hersteller und ggf. Preis der Kunde vorgibt.

Router planen

Bei der Planung der Router ist darauf zu achten,

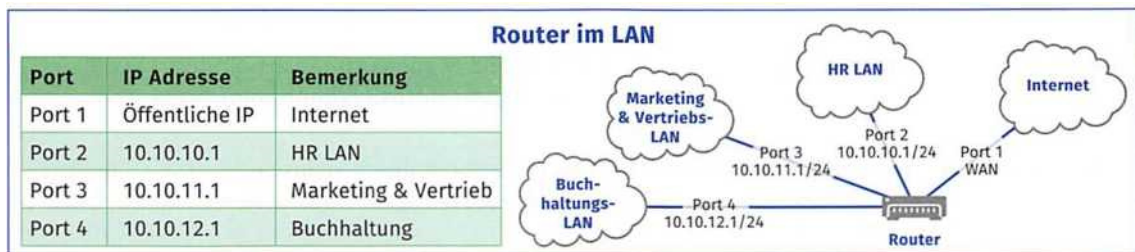
- Welche WAN-Schnittstellen unterstützt werden müssen (Glasfaser, LTE, VDSL),
- welche Datendurchsatzraten für das LAN unterstützt werden sollen, wie viele VLANs und VPNs unterstützt werden sollen,
- Wie viele Netzwerk-Ports benötigt werden,
- ob Software Defined WAN (SD WAN) inklusive Multiprotocol Label Switching, kurz MPLS (eine spezielle Routing Technik in Telekommunikationsnetzen), zum Einsatz kommen soll,
- welche Zusatzfunktionen benötigt werden,
- welchen Hersteller/ Preis der Kunde bevorzugt.



*Glasfaser/Gigabit-Ethernet/VPN-Router 1790EF
der Aachener Firma LANCOM*

Beispiel: Router im LAN

An den Ports des Routers werden Subnetze mit entsprechende IP-Adressen gemäß der Tabelle konfiguriert.



LE 5 - Server

Server-Hardware planen

Server sind letztendlich Computer wie auch Desktop-Systeme. Unterschiede gibt es in der Performance und in den Motherboards für die entsprechenden Gehäuseformen.

Bei der Planung der Server-Hardware sind zu berücksichtigen:

- Prozessoren,
- Arbeitsspeicher,
- Schnittstellen und Anschlüsse,
- Festplattenarten,
- RAID-Level.

Serveranwendungen planen

Die folgende Liste gibt eine Übersicht über häufig genutzte Serveranwendungen in Unternehmen. Jede dieser Serveranwendungen kann auf einem eigenen Server installiert, Virtualisiert oder als Container aufgesetzt werden. Die Datenhoheit verbleibt beim Kunden. Die Lösungen verhelfen zur digitalen Souveränität.

Mit der Virtualisierung von Serveranwendungen, erhält der Kunde alle Vorteile wie skalierbare Performance, einfache Sicherung, zentrales Monitoring und Management durch den Kunden selbst oder einen Administrator (Dienstleister) des Vertrauens. Die folgende Tabelle gibt einen Überblick, welche Open-Source-Serveranwendungen bereits heute produktiv in Unternehmen eingesetzt werden.

Open-Source-Serveranwendungen		
Serveranwendung	Anwendungsfall	Lizenz
BigBlueButton™	Virtuelles Klassenzimmer (erweitertes Videokonferenz-System) auf Basis html5 und WebRTC (https://github.com/bigbluebutton/bigblue-button)	LGPL
Cryptpad	Anwendungssuite für die vertrauliche Zusammenarbeit mit Ende- zu-Ende-Verschlüsselung mit Rich Text, Tabellen, Code/Markdown, Kanban, Präsentationen, Whiteboard, Umfragen (https://github.com/xwiki-labs/cryptpad)	AGPL
Debian	Debian stellt Server- und Desktop-Betriebssysteme auf Basis von Linux bereit (https://www.debian.org)	Free Software
JasperReports	Reporting Server, Business Intelligence Lösung (https://community.jaspersoft.com)	AGPL
Mattermost	webbasiertes Instant-Messaging, ähnlich Microsoft Teams oder Slack (https://github.com/mattermost/mattermost-server)	MIT + AGPL
Mautic	E-Mail-Marketing inklusive Kontaktverwaltung, Lead Management, Landing Pages und Kampagnen (https://github.com/mautic/mautic)	GPLv3
metasfresh	Open-Source-ERP inklusive CRM, Produkt- und Auftragsverwaltung, Bestellwesen, Fakturierung und Lieferung (https://github.com/metas-fresh/metasfresh)	GPL
Nextcloud	webbasierte Plattform zum Austausch von Dateien inklusive Adressbuch, Kalender, Kanban Boards, Office, Umfragen, Videokonferenzen (https://nextcloud.com)	AGPLv3
SuiteCRM	Kundenmanagement-Lösung/Customer Relationship Management (https://github.com/salesagility/SuiteCRM)	AGPL
Ubuntu	Server- und Desktop-Betriebssysteme auf Basis „debian Linux“ (https://ubuntu.com/download/server)	GPL

LE 6 - Nicht funktionale Anforderungen planen

Auch die Planung nicht funktionaler Anforderungen spielt bei der Erstellung des Pflichtenheftes eine Rolle. Da Open-Source-Serveranwendungen immer häufiger in Unternehmen eingesetzt werden, werden zuerst die Open-Source-Lizenzen genauer betrachtet.

Open-Source-Lizenzen

Beim Einsatz von Produkten sind die Lizenzbestimmungen zu berücksichtigen und im Pflichtenheft zu dokumentieren. So besitzen nicht nur proprietäre, nicht einsehbare Software (Closed Source) Lizenzbestimmungen, sondern auch Open Source. Freie Software (Free Software) besitzt keinerlei Einschränkungen, was die Nutzungsrechte betrifft.

Free Software

Bei dem Konzept der Free Software (Freie Software) werden einem Nutzer mit dem Empfang der Software, d.h. dem Kauf, Download, Bereitstellen etc., die Nutzungsrechte nicht vorenthalten oder anderweitig beschränkt. Zu den Freiheiten zählen beispielsweise der Zugang zum Quellcode für Änderungen und Analysen oder das Recht, die Software im Original oder verändert zu kopieren usw. Das Konzept der Free Software (siehe Free Software Foundation, www.fsf.org) steht also im Gegensatz zur proprietären Software. Ein Beispiel für Free Software ist das Server-Betriebssystem „debian“.

Da mit jedem geschaffenen Software-Werk eine Absicht verfolgt wird, obliegt es den Entwicklern, welche Lizenz zum Einsatz kommen soll. Die folgende Tabelle zeigt die am häufigsten genutzten Open-Source-Lizenzen:

Open-Source-Lizenzen	
AGPL	Die GNU Affero General Public License baut auf GPL auf, schließt aber eine Lücke des GPL: Sie verpflichtet Service-Provider, Änderungen an der AGPL-Software ebenfalls als Quelltext weiterzugeben.
Open Source	Die Open-Source-Initiative veröffentlicht Lizenzen, die eine freie Nutzung, Änderung und Weitergabe von Software ermöglichen. Folgende Lizenzen haben den Lizenzprüfungsprozess erfolgreich durchlaufen (Stand: 2021): Apache License 2.0, BSD 3-Clause "New" or "Revised" license, BSD 2-Clause "Simplified" or "FreeBSD" license, GNU General Public License (GPL), GNU Library or "Lesser" General Public License (LGPL), MIT license, Mozilla Public License 2.0, Common Development and Distribution License, Eclipse Public License version 2.0.

Rechtliche und organisatorische Vorgaben

Als nicht funktionale Kriterien in der Beschaffung von Netzwerkkomponenten und Systemen sind insbesondere auch rechtliche und organisatorische Aspekte zu berücksichtigen. Für öffentliche Auftraggeber ist die Einhaltung rechtlicher Vorgaben zwingend, will man nicht Konkurrenz- und Schadensersatzklagen bewirken. Alle Unternehmen müssen nicht funktionale Anforderungen einhalten, um eine hohe Akzeptanz bei Bietern einzuhalten, möglichst viele attraktive Angebote zu erhalten und Compliance-Anforderungen einzuhalten. Alle Beteiligten der Projekte sind daher aufgefordert, sich auch mit nicht funktionalen Anforderungen auseinanderzusetzen. Insbesondere die kaufmännischen IT-Berufe bearbeiten die Ausschreibungsverfahren federführend.



Weitere Anforderungen

Die folgende Tabelle gibt eine Übersicht, welche weiteren nicht funktionalen Anforderungen im Pflichtenheft dokumentiert werden.

Weitere Anforderungen	
Anforderungen	Beschreibung
Performance-Anforderungen	siehe auch Jahrgangsband 1, Lernfeld 2
Skalierbarkeit	siehe auch Jahrgangsband 1, Lernfeld 2, Kapitel 2.4.13, Abschnitt (3) und Lernfeld 9, Kapitel 9.1.1
Anwendungsmonitoring	Das Anwendungsmonitoring dient dem Kunden, während das Systemmonitoring dem Administrator dient
Systemverfügbarkeit	siehe auch Jahrgangsband 1, Lernfeld 3, Kapitel 3.8.4, Lernfeld 6, Kapitel 6.2.3 sowie Lernfeld 9, Kapitel 9.1.1 und 9.3.3
Supportzeiten und Wartungsfenster	siehe auch Jahrgangsband 1, Lernfeld 6, Kapitel 6.3.3
Datensicherung und Wiederherstellung	Während in den funktionalen Anforderungen die technische Umsetzung von Datensicherung und Wiederherstellung beschrieben wird, beschreibt dieser Abschnitt, was genau wie und wie oft und zu welchen Zeitpunkten gesichert werden soll.
Reporting	siehe auch Jahrgangsband 1, Lernfeld 6, Kapitel 6.2.3 und 6.3.3

TAG 13 - Netzwerke installieren, konfigurieren und bereitstellen

Zur Installation und Konfiguration von Netzwerken gehören das Einrichten der Infrastruktur, die Installation von Netzwerkkomponenten und die Installation von Servern. Die folgenden Kapitel beschreiben die jeweiligen Tätigkeiten, die dabei anfallen.



LE 1 - Infrastruktur einrichten

Zur Einrichtung der Infrastruktur gehören das Verlegen der Netzwerkkabel, der Anschluss der Netzwerkdosen und der Patch Panel. Für diese Tätigkeiten sind spezielle Werkzeuge erforderlich. Das folgende Werkzeugset zeigt die wichtigsten Werkzeuge: (1) LSA Auflegewerkzeug, (2) Mini-Messer, (3) Abisolierer für Koaxialkabel, (4) Crimpzange, (5) Abisolierer für Netzwerkkabel, (6) Netzwerkkabel-Tester.



Verlegen von Netzwerkkabeln

Beim Verlegen von Netzwerkkabeln kommen Cat5e-/Cat6-/Cat7-Netzwerkkabel zum Einsatz. Für die Buchsen und Stecker haben sich in der Praxis für alle Kabel RJ45-Stecker durchgesetzt. Netzwerkkabel werden von den Netzwerkdosen der Büros zu einem zentralen Anschlussraum verlegt. Das ist typischerweise der Raum, indem sich der WAN-Anschluss befindet.

Netzwerkkabel verlegen

Netzwerkkabel werden in Kabelkanälen verlegt. Jede Netzwerkdose in den Büros erhält ein eigenes Kabel bis zum Anschlussraum. Soll beispielsweise ein Arbeitsplatz einen Desktop-Computer und einen Netzwerkscanner erhalten, so sind an diesem Arbeitsplatz zwei Netzwerkbuchsen erforderlich und je ein Kabel von jeder Netzwerkdose zum Anschlussraum, bzw. bis zum nächsten Switch.



19-Zoll-Rack in einem Anschlussraum mit zwei Cat6-Patch-Panels und zwei Switches

Kabelkanäle bieten den Vorteil, dass auch nachträglich noch Netzwerkkabel hineingelegt werden können. Lassen sich keine Kabelkanäle einsetzen, so sollten Leerrohre eingesetzt werden. Auch diese ermöglichen ein späteres, nachträgliches Einziehen von Netzwerkkabeln.

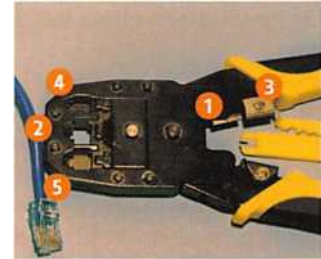
Im Anschlussraum laufen die Netzwerkkabel zusammen und werden in einem Patch Panel zusammengeführt, siehe Bild oben im Kasten.

Crimpen von Netzkabeln



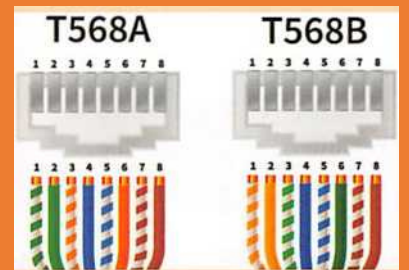
Bei den Netzwerksteckern haben sich RJ45-Stecker und -Buchsen etabliert. Für das Aufstecken der RJ45-Stecker auf die Enden von Netzkabeln werden neben dem Netzkabel für jedes Kabelende ein Knickschutz, ein RJ45-Stecker und ggf. eine Einfädelhilfe (siehe nebenstehende Abbildung) benötigt.

Zudem wird eine Crimpzange benötigt. Mit dem Messer (1) werden Kabel in der gewünschten Länge abisoliert. Die Crimpzange im Bild rechts kann 4-polige (4), 6-polige (5) und 8-polige RJ-Stecker (2) crimmen. Für das Aufstecken und Crimpen von RJ45 werden 8-polige Stecker (2) genutzt. Mit der Schneide (3) werden einzelne Adern gekürzt.

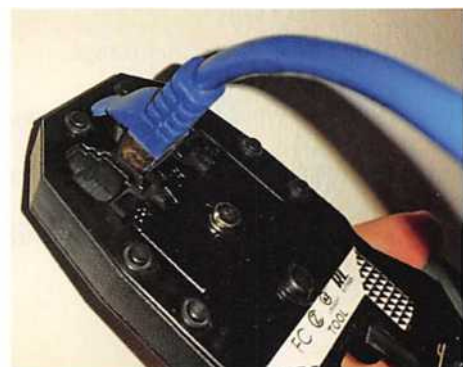


Auf das Ende des Netzkabels wird zuerst der Knickschutz aufgesteckt. Anschließend wird das Netzkabel ca. 2 cm abisoliert. Die Abschirmung darf nicht beschädigt werden. Die Abschirmung bzw. das Drahtgeflecht wird schließlich nach hinten umwickelt. Die einzelnen Aderenden werden in die Einfädelhilfe sortiert. Anschließend wird die Einfädelhilfe in den Netzwerkstecker geführt.

Beide Enden des Netzkabels (siehe Schaubild) werden nach TIA 568-A belegt oder aber beide Enden nach TIA 568-B (Bild rechts).



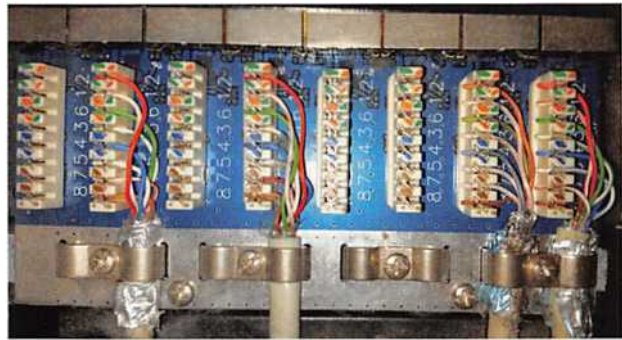
Pin	Pin-Belegung nach TIA568-A	Pin-Belegung nach TIA568-B
1	Green	Orange
2	White	White
3	Blue	Green
4	White	White
5	Orange	Blue
6	White	White
7	Brown	Brown
8	White	White



Beim Zusammendrücken der Crimpzange werden die acht einzelnen Aderenden in den Stecker gedrückt (links). Der RJ45-Stecker wird samt Kabel in die Crimpzange eingelegt (rechts).

Installation eines Patch Panels

Im Anschlussraum laufen alle Netzkabel der Büros zusammen. Die Netzkabelenden werden abisoliert und die acht einzelnen Aderenden eines jeden Kabels mit dem LSA-Anlegewerkzeug in die entsprechende farblich kodierte Position des Patch Panels gedrückt. LSA steht für die verwendete Schneidklemmtechnik. Sie ist lötfrei, schraubfrei und abisolierfrei (Isa).



Patch Panel mit vier aufgelegten Netzkabeln

Wichtig ist, dass beide Enden der Netzkabel in der gleichen Reihenfolge verdrahtet bzw. „aufgelegt“ werden, also entweder beide Enden nach TIA 568-A oder beide Enden nach TIA 568-B.

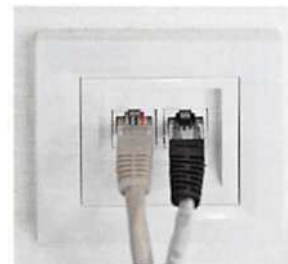


LSA Anlegewerkzeug für Patch Panels

Die Anschlüsse und welcher Port zu welcher Netzwerkdose gehört, werden dokumentiert!

Installation von RJ45-Netzwerkdosen

Bei der Installation der Netzwerkdosen wird die Pin-Belegung des Patch Panels übernommen. Wurde die bisherige Verdrahtung nach TIA 568-A durchgeführt, dann werden auch alle Netzwerkdosen nach TIA-568-A durchgeführt. Alternativ können alle Patch Panels und Netzwerkdosen der TIA 568-B folgen. Die einzelnen Aderenden werden mit dem LSA-Anlegewerkzeug auf die Kontakte der Rückseite gedrückt.



RJ45-Netzwerkdose

LE 2 - Netzwerkkomponenten installieren

Welche Komponenten bei der Installation eines Netzwerkes tatsächlich zum Einsatz kommen, hängt von den Kundenanforderungen ab.

Beispiel: Router installieren

Da in jedem Kundenumfeld ein Router zum Einsatz kommt, beschreibt dieser Abschnitt exemplarisch die Installation eines Routers. Vor der Installation erfolgt die Auswahl des Routers.

Die Auswahl des Routers hängt im Wesentlichen von der Größe des Netzwerks und somit von der Unternehmensgröße des Kunden ab:

- Für die Absicherung von Netzwerken großer Unternehmen bietet sich eine Next-Generation-Router-/Firewall-Lösung an, z.B. die Open-Source-Lösung „OPNsense®“ auf einer x86-64-Plattform (<https://opnsense.org>). Diese Lösung ist als Software und ebenso als Hardware verfügbar.
- Für kleinere und mittlere Firmen reicht oftmals eine Fritz!Box. Für Glasfaser stehen die Fritz!Box 5490 für aktive Glasfasernetzwerke (AON) und die Fritz!Box 5491 für passive Glasfasernetzwerke (GPON), für DSL die Fritz!Box 7590 und für Kabel die Fritz!Box 6660 zur Verfügung.

Dieser Abschnitt beschreibt exemplarisch die Installation einer Fritz!Box 7590 an einem DSL-Anschluss, weil sie einen hohen Verbreitungsgrad in Deutschland besitzt. Über die vier LAN-Buchsen (schwarzes, weißes, grünes, weißes Netzkabel, siehe Abbildung) lassen sich bis zu vier Buchsen des Patch Panels verbinden. Werden mehr Buchsen benötigt, so ist ein Switch dazwischenschalten. Alternativ kann die blaue WAN-Buchse (siehe Abbildung) als LAN5 konfiguriert werden.



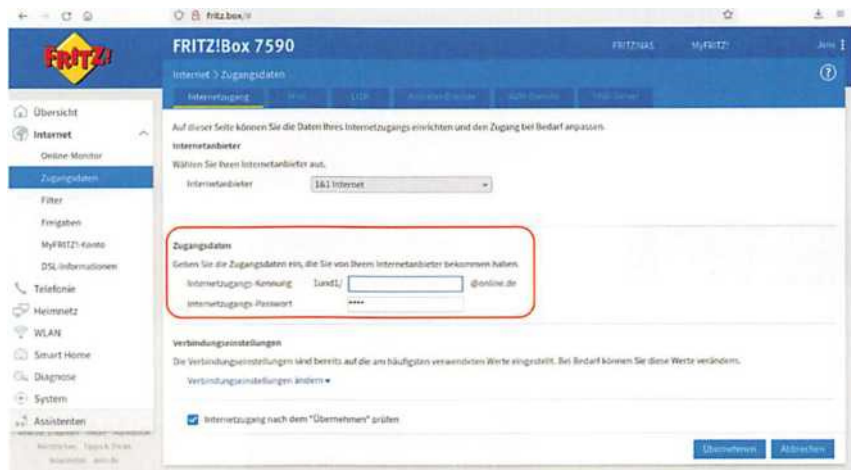
Rückseite einer Fritz!Box 7590, beigefarbener Stecker in der grauen DSL-Buchse (links)



Über den Menüpunkt „Internet – Zugangsdaten“ lassen sich die Zugangsdaten des Anbieters (hier: DSL-Anbieter) eintragen.

Nach Einschalten der Fritz!Box ist diese über die IP-Adresse 192.168.178.1 bzw. über die Browser-URL <http://192.168.178.1> und alternativ über <http://fritz.box> erreichbar. Das Passwort ist auf der Rückseite der Fritz!Box aufgedruckt.

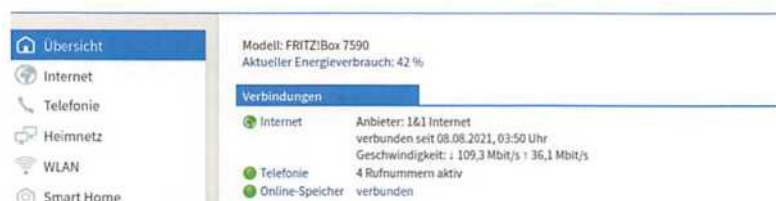
Nach dem Login stellen wir die Ansicht auf „Erweiterte Ansicht“ um (siehe nebenstehende Abbildung).



Weitere Einstellungen:

- Im Reiter IPv6 lässt sich die IPv6-Unterstützung aktivieren, wenn diese gewünscht ist.
- Im Reiter LISP lässt sich das Locator/ID Separation Protocol (LISP) aktivieren (siehe RFC6839, <https://datatracker.ietf.org/doc/html/rfc6830>).
- Im Reiter DNS-Server lässt sich DNS over TLS aktivieren, wenn eine abhörsichere/verschlüsselte Namensauflösung gewünscht ist.

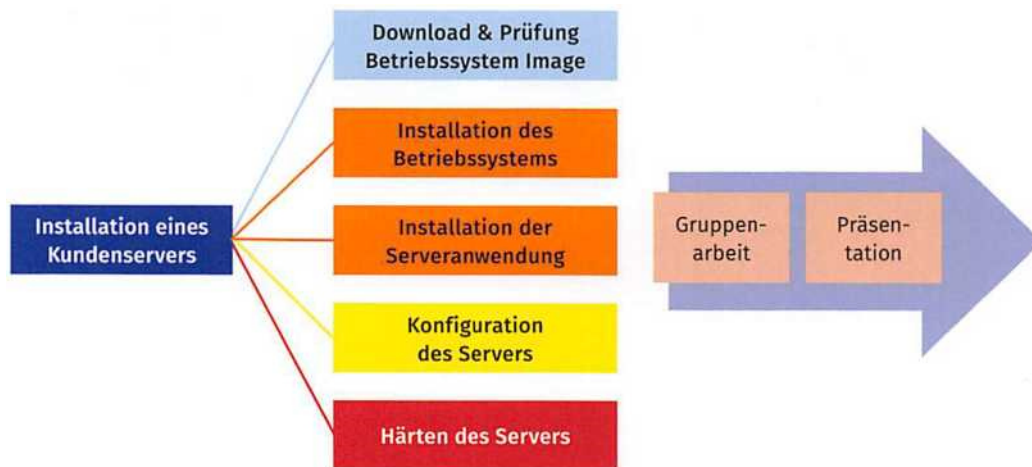
Nach dem Klicken auf "Übernehmen" benötigt es ein paar Minuten, bis die Verbindung zum Internet aufgebaut ist.



Wie abgebildet hat der Router die Verbindung zum Internet hergestellt. Die vier Rufnummern wurden über den Menüpunkt „Telefonie“ konfiguriert.

LE 3 - Server installieren (klassisch)

Dieser Abschnitt beschreibt die Installation eines Bare-Metal-Servers. Die klassische Vorgehensweise beinhaltet folgende Schritte:



Die gewünschte Server-Anwendung des Kunden gibt vor, welche Betriebssysteme unterstützt werden und welches eingesetzt werden kann. Die folgenden Abschnitte beschreiben die einzelnen Schritte aus dem Schaubild.

In diesem Abschnitt wird exemplarisch die Kundenanforderung „Installation und Betrieb einer firmeninternen Nextcloud auf einem Bare Metal des Kunden“ umgesetzt.

Nextcloud

Bei der Nextcloud handelt es sich um eine Groupware, eine webbasierte Software für die Zusammenarbeit in Teams. So bietet Nextcloud eine Dateiaustauschplattform, Messaging, Videokonferenz, Kanban Boards, Umfragen, Kalender, Adressbücher, Office- Paket etc. Alle Anwendungen lassen sich über den Browser bedienen.

Auf <https://apps.nextcloud.com/> gibt es eine Vielzahl an

Server- Apps, mit denen der eigene Next-Cloud-Server erweitert werden kann. Es gibt entsprechende Apps für Smartphones, z. B. auf <https://f-droid.org/>. Damit können Smartphones auf den eigenen Nextcloud-Server zugreifen, um Dateien, Adressen, Termine zu synchronisieren, Fotos hochzuladen oder Dokumente herunterzuladen.



Mit einer Nextcloud lässt sich Zusammenarbeit im Team in der eigenen Cloud umsetzen.

Download und Prüfung des Betriebssystem-Images

In der Nextcloud-Dokumentation finden sich Systemanforderungen (https://docs.nextcloud.com/server/latest/admin_manual/installation/system_requirements.html) für das empfohlene Betriebssystem: Wir wählen Ubuntu 20.04 LTS. Die Server-Images finden sich auf <https://ubuntu.com> (*Download - Ubuntu Server-Get Ubuntu Server - [Option 2 - Manual server installation]*). Es müssen drei Dateien heruntergeladen werden:

Ubuntu-Server-Image	
Beschreibung	Download URL
Installationsdatei als ISO-Image; wird nach der Prüfung auf ein USB-Stick oder eine DVD gebrannt	https://releases.ubuntu.com/20.04/ubuntu-20.04.2-live-server-amd64.iso
Prüfsumme des ISO-Image	https://releases.ubuntu.com/20.04/SHA256SUMS
Schlüssel zum Überprüfen	https://releases.ubuntu.com/20.04/SHA256SUMS.gpg

Nach dem Download der ISO-Datei wird diese auf Korrektheit und Authentizität überprüft. Die Datei „SHA256SUMS“ enthält die Prüfsumme, die mit dem Werkzeug „sha256sum“ nachgerechnet werden kann. Für das Ubuntu Image ist der Inhalt dieser Prüfsummendatei der folgende:

</> Ausgabe der Datei SHA256SUMS für Ubuntu 20.04.2 im Terminal

```
cat SHA256SUMS

d1f2bf834bbe9bb43faf16f9be992a6f3935e65be0edece1dee2aa6eb1767423
*ubuntu-20.04.2-live-server-amd64.iso
93bdab204067321ff131f560879db46bee3b994bf24836bb78538640f689e58f
*ubuntu-20.04.2.0-desktop-amd64.iso
```

Die Überprüfung der iso-Datei auf Korrektheit geschieht unter Linux wie folgt:

</> Überprüfen der ISO-Datei im Terminal

```
echo "d1f2bf834bbe9bb43faf16f9be992a6f3935e65be0edece1dee2aa6eb1767423
*ubuntu-20.04.2-live-server-amd64.iso" | shasum -a 256 -check

ubuntu-20.04.2-live-server-amd64.iso: OK
```

Die Ausgabe von OK bescheinigt, dass die errechnete Prüfsumme identisch ist mit der Prüfsumme in der Datei „SHA256SUMS“. Nun muss noch geprüft werden, ob die Prüfsummendatei an sich authentisch ist.

</> Überprüfen der Signatur im Terminal

```
gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS

gpg: Signatur vom Do 11 Feb 2021 20:07:58 CET
gpg:           mittels RSA-Schlüssel 843938DF228D22F7B3742BC0D
94AA3F0EFE21092
gpg: Korrekte Signatur von «Ubuntu CD Image Automatic Signing Key (2012)
<cdimage@ubuntu.com>» [unbekannt]
gpg: WARNUNG: Dieser Schlüssel trägt keine vertrauenswürdige Signatur!
gpg:           Es gibt keinen Hinweis, dass die Signatur wirklich dem
vorgeblichen Besitzer gehört.
Haupt-Fingerabdruck = 8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092
```

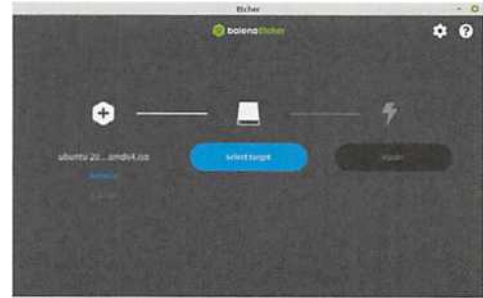
Die Zeile „Korrekte Signatur“ besagt, dass die überprüfte Datei tatsächlich vom Eigentümer der Schlüsseldatei stammt.

Eine ausführliche Dokumentation zur Überprüfung der ISO-Datei findet sich hier <https://ubuntu.com/tutorials/how-to-verify-ubuntu#1-overview>.

Installation des Betriebssystems

Die ISO-Datei kann nun auf eine DVD gebrannt oder über einen Image-Writer auf einen USB-Stick kopiert werden. Die Open Source „balenaEtcher“ ermöglicht das Kopieren auf einen USB-Stick (siehe nebenstehende Abbildung, <https://www.balena.io/etcher/>).

Mit dem bootfähigen USB-Stick oder der bootfähigen DVD wird der Server gestartet und installiert.



Nach der Installation wird die Betriebssystemversion im Terminal wie folgt geprüft:

Überprüfen der Serverinstallation

```
lsb_release -a

No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 20.04.2 LTS
Release: 20.04
Codename: focal
```

Die Installation des Serverbetriebssystems ist fast abgeschlossen. Für einen Server ist es angebracht, Sicherheitsupdates automatisch zu installieren. Dies geschieht über die Installation der unattended-upgrades.

Unattended-upgrades einrichten

```
sudo apt install unattended-upgrades
dpkg-reconfigure -pflow unattended-upgrades
```

Installation der Serveranwendung

Die folgende Abbildung zeigt einen Ausschnitt möglicher Serverdienste, die bei der Ubuntu-Serverinstallation mit einem Klick als Snap installiert werden können. Das ist eine Variante zur Installation einer Nextcloud-Serveranwendung:



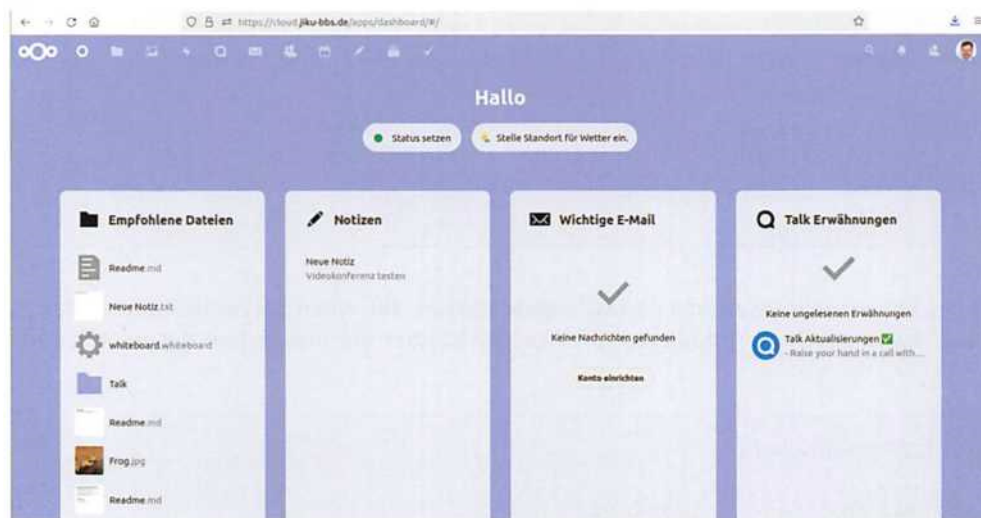
Installation von Nextcloud auf einem Ubuntu-Server

Varianten	Beschreibung
snap	Nextcloud als Snap-Package installieren über <code>sudo snap install nextcloud</code>
docker	Docker einrichten und das aktuelle docker-Image von https://hub.docker.com herunterladen und starten über <code>docker pull nextcloud</code>
vm	QEMU/KVM installieren, eine virtuelle Maschine einrichten, das Installationskript https://github.com/nextcloud/vm/blob/master/nextcloudinstall_production.sh herunterladen und in der VM ausführen über <code>sudo bash nextcloud_install_production.sh</code>

Alle drei Varianten führen den Nextcloud-Server in einer sicheren "Sandbox"-Umgebung aus und erlauben zudem, weitere Webanwendungen parallel zu betreiben. Wir führen exemplarisch eine lokale Installation über das Installationskript „nextcloud_install_production.sh“ durch.

Konfiguration des Servers

Nach der Installation lässt sich der Nextcloud-Server über den Browser aufrufen und konfigurieren.



Konfiguration der Nextcloud

Der Server lässt sich über den Browser administrieren, konfigurieren, erweitern und aktualisieren. Oben rechts über das kreisrunde Icon (eigenes Profilbild) befindet sich das Menü.

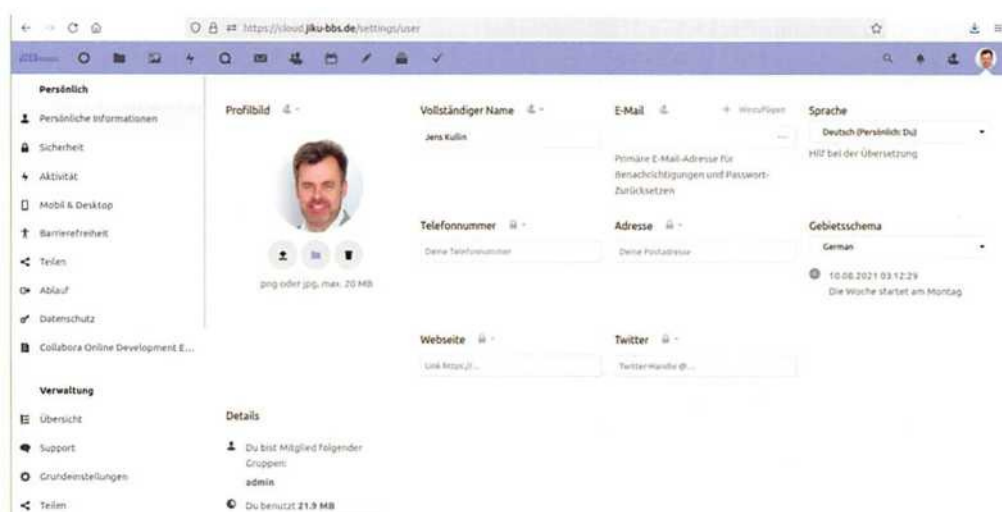
Über Einstellungen kann z.B. ein Profilbild hochgeladen werden.

Über Apps können weitere Apps auf den Nextcloud-Server installiert werden, z.B. Circles für die Zusammenarbeit in Gruppen, Calendar, Deck für Kanban Boards, Draw.io, MindMap, OnlyOffice, Polls für Umfragen, Talk für Messaging, Tasks, User Account Deletion, Whiteboard Integration.

Über Benutzer können weitere Anwender eingerichtet werden. Vorab sollte allerdings ein E-Mail-Server für ausgehende E-Mails konfiguriert werden.

Profil konfigurieren

Über das Menü oben rechts (*Einstellungen*) gelangt der Anwender in das eigene Profil: Hier lässt sich ein Profilbild hochladen, die Sprache auf *Deutsch* und das Gebietsschema auf *German* setzen.



LE 4 - E-Mail-Server für den Nachrichtenversand konfigurieren

In der Navigation Links über die Grundeinstellungen sollte ein bereits vorhandener E-Mail-Account eingerichtet werden. Diesen nutzt der Server, um Benachrichtigungen zu versenden. Geeignet ist z.B. eine „info@“-E-Mail-Adresse. Nach der Konfiguration des E-Mail-Server kann dieser über den Knopf unten „E-Mail senden“ getestet werden.

E-Mail-Server *i*

Es ist wichtig diesen Server so zu konfigurieren, dass E-Mails versandt werden können, z.B. für den Passwort-Reset und Benachrichtigungen.

Sendemodus: SMTP | Verschlüsselung: SSL/TLS

Absenderadresse: @

Authentifizierungsmethode: Anmelden | ☒ Authentifizierung benötigt

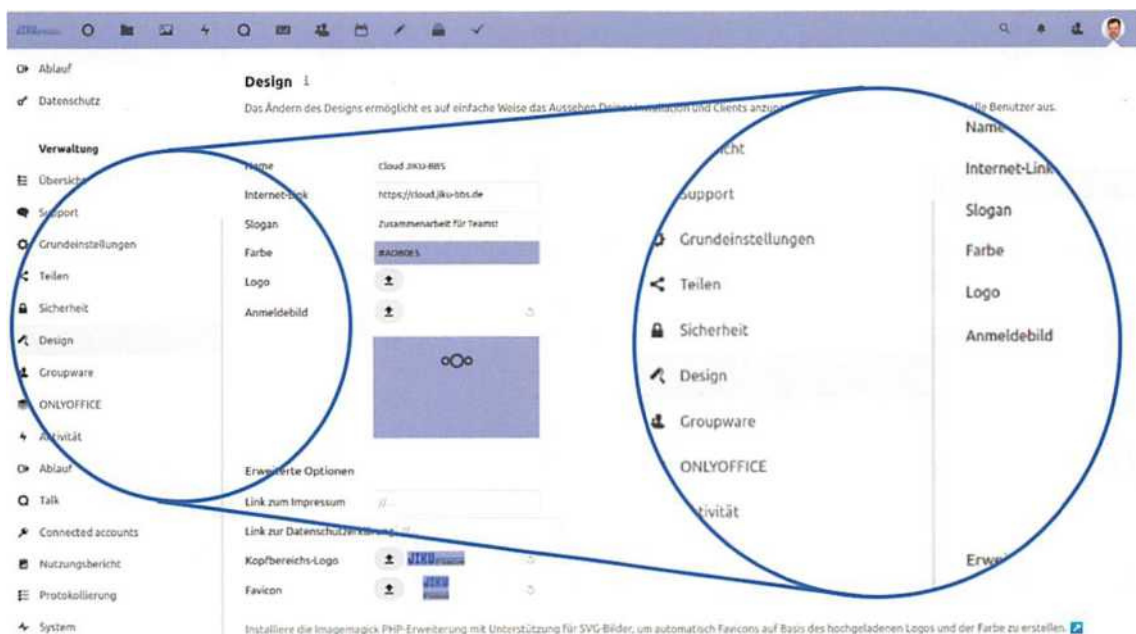
Serveradresse: : 465

Zugangsdaten:

E-Mail-Einstellungen testen

Design der Weboberfläche konfigurieren

Ebenfalls in der Navigation findet sich unterhalb von *Sicherheit* der Punkt „Design“: hier können die Farben und URLs angepasst, ein Link zum Impressum und zur Datenschutzerklärung hinterlegt und ein Logo eingebunden werden.



Anleitungen für Nextcloud

Es gibt verschiedene Nextcloud-Hilfen im Internet. Diese sind zumeist in englischer Sprache, enthalten oft aber alle Antworten!

Benutzerhandbuch: https://docs.nextcloud.com/server/22/user_manual/en

Administrationshandbuch: https://docs.nextcloud.com/server/22/admin_manual

Hilfeforen: <https://help.nextcloud.com>

LE 5 - Härten des Servers

Um die Sicherheit von Servern zu erhöhen, werden diese „gehärtet“. Hierunter fallen alle Maßnahmen, um Angriffsmöglichkeiten zu minimieren, z.B. das Abschalten nicht benötigter Dienste, das regelmäßige Installieren von Updates (Patches) etc. Das Härten eines Ubuntu-basierten Servers läuft über das Terminal, z. B. über ssh.

Härten des Servers

- Härten der Anwendung gemäß Anleitung unter https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html
- Installieren einer Firewall (sudo apt install ufw), Schließen aller eingehenden Ports bis auf 80/tcp und 443/tcp für den Webzugang und 22/tcp für den ssh-Zugang
- Regelmäßige Prüfung sicherheitsrelevanter Ereignisse in der Nextcloud (*Verwaltung - Übersicht*)



Uncomplicated Firewall ufw in ubuntu einrichten

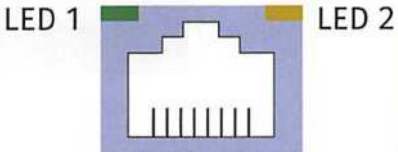
```
sudo su
apt install ufw
ufw allow 80/tcp
ufw allow 443/tcp
ufw allow 22/tcp
ufw default deny incoming
ufw enable
systemctl restart ufw
ufw status
```

TAG 14 - Funktionsprüfungen und Messungen durchführen, Dokumentationen erstellen

Nach der jeweiligen Installation von Infrastruktur, Netzwerkkomponenten und Server müssen diese auf Funktion überprüft werden. Dazu gibt es verschiedene Werkzeuge.

LE 1 - Prüfung der Infrastruktur

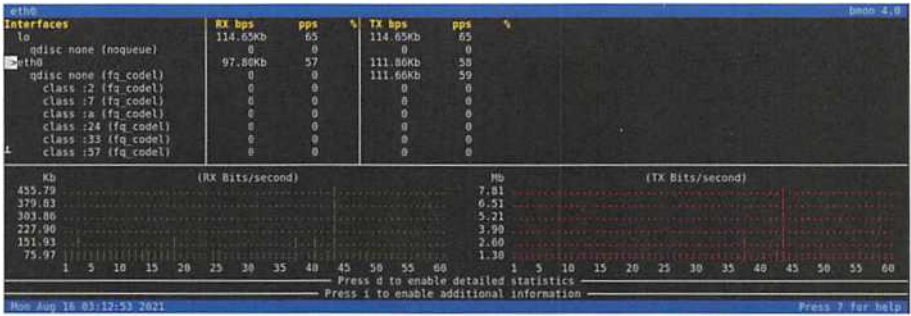
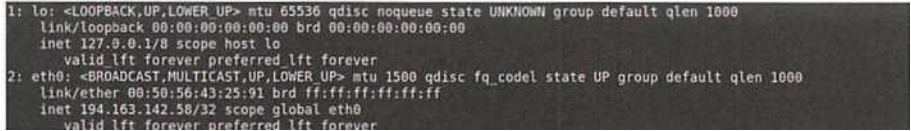
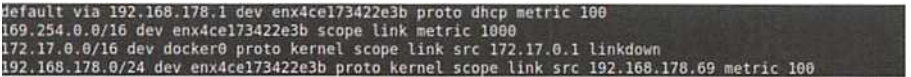
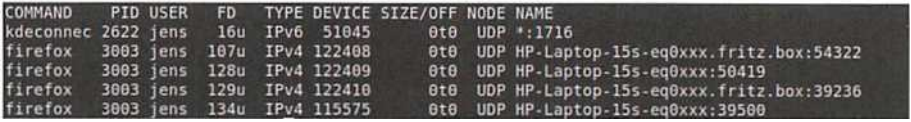
Nach der Installation der Infrastruktur muss diese überprüft werden. Dafür können verschiedene Hilfsmittel herangezogen werden. Die folgende Tabelle gibt eine Übersicht dazu.

Hilfsmittel zur Prüfung der Infrastruktur	
Hilfsmittel	Bedeutung
Kabeltester	Mit einem Kabeltester ist es möglich, ein komplettes Netzkabel zu überprüfen. Dazu werden beide Enden des Netzkabels in das Messgerät gesteckt und der Test gestartet. Nacheinander leuchten links und rechts jeweils die LED 1, LED 2, LED 3 etc. auf. Das Netzkabel ist in Ordnung, wenn alle acht LEDs synchron links und rechts aufleuchten. Die neunte LED G steht für Ground (Masse). Besonderheit: Bei einem Crosskabel sind mehrere Pins vertauscht. Solche Netzkabel sollten entsprechend gekennzeichnet werden. Mit zwei bereits geprüften Netzkabeln lässt sich die Verbindung der Netzdosen zum Patch Panel überprüfen. 
Netzbuchsen	Netzbuchsen verfügen über zwei Status-LEDs. Die grüne LED leuchtet bzw. blinkt, wenn eine Verbindung vorhanden ist. Die gelbe LED zeigt zusätzlich die Geschwindigkeit an. 

LE 2 - Prüfung der Netzwerkkomponenten

Bei den hier vorgestellten wichtigen Werkzeugen zur Prüfung von Netzwerkkomponenten handelt es sich um Software, die in der Shell (Kommandozeile) auf Linux-Systemen ausgeführt werden. Sie funktionieren auf Linux-Desktops und Linux-Servern. Die einzelnen Kommandos sind jeweils ohne in die jeweilige Shell einzugeben.

Prüfung von Netzkomponenten	
Werkzeug	Bedeutung mit Beispielen
arp	Über das Kommando „arp“ werden die Nachbarn im Netzwerk ausgegeben <pre>Adresse Hardware-Typ Hardware-Adresse Optionen Maske Schnittstelle 192.168.178.240 ether 1e:5a:26:fd:44:51 C enx4ce173422e3b nextcloudpi.fritz.box ether b8:27:eb:a7:a2:cd C enx4ce173422e3b</pre> Im Beispiel wurden zwei Nachbarn im Netzwerk gefunden.

Prüfung von Netzkomponenten	
Werkzeug	Bedeutung mit Beispielen
bmon	Mit dem Kommando „bmon-b“ kann in der Shell der aktuelle Netzwerkverkehr ausgegeben werden.  Im Beispiel wurde die Netzwerkschnittstelle „eth0“ ausgewählt. Im unteren Bereich wird angezeigt, welcher Netzwerk-Traffic aktuell darüber läuft.
ip address	Das Kommando „ip address“ in einer Linux Shell gibt aus, welche Netzwerkschnittstellen vorhanden und wie diese konfiguriert sind.  Die obige Ausgabe zeigt, dass es ein Loopback Adapter - die IP-Adresse 127.0.0.1 (auch als localhost bezeichnet) - und eth0 gibt. eth0 hat die IP-Adresse 194.163.142.58/32 zugewiesen bekommen.
ip neighbor show	Über das Kommando „ip neighbor show“ werden die Nachbarn im Netzwerk ausgegeben.  Im Beispiel wurden zwei Nachbarn gefunden.
ip route	Das Kommando „ip route“ zeigt die aktuellen Routen an. 
lsof	Mit der Software „lsof“ werden nicht nur offene Dateien aufgelistet („list open files“), es lassen sich damit auch Netzwerkverbindungen anzeigen. Die Eingabe von „lsof-i tcp“ zeigt beispielsweise alle offenen TCP-Verbindungen an.  Im Beispiel horcht die lokale Anwendung „kdeconnect“ auf den TCP-Port 1716, die Anwendung „AppRun“ hält eine TCP-Verbindung zur Netzwerkkomponente „nextcloudpi.fritz.box“. Die Eingabe von „lsof-i udp“ zeigt alle offenen UDP-Verbindungen an:  Im Beispiel horcht die Anwendung „kdeconnect“ auf den UDP-Port 1716. Die Anwendung Firefox horcht auf den UDP-Ports 54322, 50419, 39236 und 39500.

Prüfung von Netzkomponenten	
Werkzeug	Bedeutung mit Beispielen
nmcli	Mit dem NetworkManager Command Line Interface lässt sich der Linux-Netzwerk- Manager in der Shell nutzen. Der Befehl „nmcli device“ zeigt eine Kurzübersicht aller Netzwerkadapter: <pre> DEVICE TYPE STATE CONNECTION enx4ce173422e3b ethernet verbunden Kabelgebundene-Verbindung 1 docker0 bridge verbunden docker0 wlo1 wifi nicht verfügbar -- lo loopback nicht verwaltet -- </pre> Der Aufruf von „nmcli“ ohne weitere Parameter zeigt die Netzwerkadapter in langer Form an. <pre> enx4ce173422e3b: verbunden zu Kabelgebundene-Verbindung 1 "Realtek RTL8153" ethernet (r8152), 4C:E1:73:42:2E:3B, hw, mtu 1500 ip4-Vorgabe inet4 192.168.178.69/24 route4 0.0.0.0/0 route4 192.168.178.0/24 route4 169.254.0.0/16 inet6 fe80::e022:d9bc:318b:1d7f/64 route6 fe80::/64 docker0: verbunden zu docker0 "docker0" bridge, 02:42:2D:36:45:AC, sw, mtu 1500 inet4 172.17.0.1/16 route4 172.17.0.0/16 </pre> Der Aufruf von „nmcli connection“ zeigt alle physikalischen Verbindungen an: <pre> NAME UUID TYPE DEVICE Kabelgebundene-Verbindung 1 826eb5eb-1a9e-1844-ba54-befc9a7fc168 ethernet enx4ce173422e3b docker0 9f3e9f48-ecad-4101-a40a-135ae66b6ebf bridge docker0 Automatisch AP JK 8671 af40c1b6-6e5b-4a21-b40a-4f87016f6a36 wifi -- </pre>
netstat	Mit der Software „netstat“ können Netzwerkstatistiken ausgegeben werden. So zeigt das Kommando „netstat-an grep tcp“ alle TCP Verbindungen an (der senkrechte Strich ist das Pipe-Zeichen: die netstat-Ausgabe wird an den Filter „grep“ weitergeleitet): <pre> tcp 0 0 0.0.0.0:1:35309 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:53:53 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:1:631 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0:192.168.178.69:48262 192.168.178.69:48262 TIME_WAIT tcp 0 0 0.0.0.0:192.168.178.69:54418 192.168.178.69:54418 TIME_WAIT </pre> Im Beispiel werden fünf Verbindungen angezeigt, auf dreien horchen Serveranwendungen, zwei TCP-Verbindungen befinden sich im Aufbau. Eine sehr große Anzahl an TIME-WAIT-Verbindungen kann ein Indiz für eine DDOS-Attacke sein. Über den zusätzlichen Befehl watch -n 1 „netstat -nt grep TIME_WAIT wc -l“ wird im Sekundentakt gezählt, wie viele Verbindungen sich im Aufbau befinden. „netstat -r“ zeigt die Routing-Tabelle an: <pre> Kernel IP routing table Destination Gateway Genmask Flags MSS Window irtt Iface default ip-194.163.128- 0.0.0.0 UG 0 0 0 eth0 </pre>
nslookup	Mit der Software „nslookup“ wird der DNS-Server ausgegeben und die Ziel-IP- Adresse. So liefert „nslookup www.westermann.de“ folgende Ausgabe in der Shell: <pre> Server: 127.0.0.53 Address: 127.0.0.53#53 Non-authoritative answer: Name: www.westermann.de Address: 217.13.73.44 </pre> Die Eingabe von „nslookup 217.13.73.44“ liefert hingegen folgendes Ergebnis: <pre> 44.73.13.217.in-addr.arpa name = w5-44.westermann.de. Authoritative answers can be found from: </pre>

Prüfung von Netzkomponenten	
Werkzeug	Bedeutung mit Beispielen
ping	Mit der Software „ping“ wird geprüft, ob eine andere Netzwerkkomponente über das Netzwerk erreichbar ist. So liefert ein „ping www.westermann.de“ beispielsweise folgende Ausgabe in der Shell: <pre>PING www.westermann.de (217.13.73.44) 56(84) Bytes Daten: 64 Bytes von w5-44.westermann.de (217.13.73.44): icmp_seq=1 ttl=56 Zeit=25.3 ms</pre> Der Server ist erreichbar, die Antwort wurde 25,3 Millisekunden nach dem Versenden empfangen. Diese Ausgabe bedeutet, dass dieser Rechner über das Netzwerk grundsätzlich erreichbar ist.
tcpdump	Mit der Software „tcpdump“ lassen sich live die Pakete einer Netzwerkschnittstelle ausgeben. So zeigt z.B. der Befehl „tcpdump-i vmbr0“ die Pakete der virtuellen Netzwerkbridge „vmbr0“ (vmbr0 muss durch die tatsächlich vorhandene Schnittstelle ersetzt werden): <pre>tcpdump: verbose output suppressed, use -v[v]... for full protocol decode listening on vmbr0, link-type EN10MB (Ethernet), snapshot length 262144 bytes 02:16:56.864807 IP pve.fritz.box.ssh > HP-Laptop-15s-eq0xxx.fritz.box.53716: Flags [P.], seq 3507999412:350799960 0, ack 3652984126, win 501, options [nop,nop,TS val 2158246917 ecr 905145609], length 188 02:16:56.865685 IP HP-Laptop-15s-eq0xxx.fritz.box.53716 > pve.fritz.box.ssh: Flags [.], ack 188, win 501, options [nop,nop,TS val 905145634 ecr 2158246917], length 0</pre>
tracert	Mit der Software „tracert“ wird der Weg zwischen zwei Systemen dokumentiert, inklusive aller Router dazwischen. Der Aufruf von „tracert www.westermann.de“ hat folgende Ausgabe in der Shell: <pre>tracert to www.westermann.de (217.13.73.44), 30 hops max, 60 byte packets 1 fritz.box (192.168.178.1) 1.152 ms 1.482 ms 1.814 ms 2 hbb1902aihr001.versatel.de (62.214.63.89) 20.564 ms 20.619 ms 22.498 ms 3 62.214.37.221 (62.214.37.221) 15.853 ms 16.164 ms 16.358 ms 4 62.214.37.118 (62.214.37.118) 23.236 ms 23.544 ms 62.214.37.114 (62.214.37.114) 23.072 ms 5 crmber11-et-5-100.as20676.net (193.178.185.60) 24.552 ms 26.641 ms 26.719 ms 6 crmdus11-cg-10-0-2-0.as20676.net (87.234.14.167) 33.376 ms 25.599 ms 27.050 ms 7 suhlu-v9.gaertner.de (217.13.66.41) 26.898 ms 26.644 ms 27.229 ms 8 suhlu-v9.gaertner.de (217.13.66.41) 27.956 ms 28.560 ms 28.820 ms</pre> Im obigen Beispiel sind insgesamt acht Router (auch Hops genannt) zum Erreichen der Netzwerkkomponente involviert. Über den Parameter „-T-p“ kann der Ziel-Port festgelegt und getestet werden. Der Aufruf von „tracert-T-p 443 www.westermann.de“ testet den https-Zugang: <pre>tracert to www.westermann.de (217.13.73.44), 30 hops max, 60 byte packets 1 fritz.box (192.168.178.1) 0.942 ms 1.127 ms 1.262 ms 2 hbb1902aihr001.versatel.de (62.214.63.89) 24.742 ms 25.031 ms 25.065 ms 3 62.214.37.221 (62.214.37.221) 12.492 ms 12.543 ms 14.907 ms 4 62.214.37.114 (62.214.37.114) 19.054 ms 62.214.37.118 (62.214.37.118) 19.299 ms 62.214.37.114 (62.214.37.114) 19.048 ms 5 crmber11-et-5-100.as20676.net (193.178.185.60) 21.209 ms 21.228 ms 21.388 ms 6 crmdus11-cg-10-0-2-0.as20676.net (87.234.14.167) 28.157 ms 24.185 ms 24.868 ms 7 suhlu-v9.gaertner.de (217.13.66.41) 23.946 ms 25.054 ms 25.072 ms 8 fw-ext.westermann.de (217.13.73.251) 24.598 ms 22.878 ms 22.781 ms 9 w5-44.westermann.de (217.13.73.44) 25.278 ms 23.273 ms 24.615 ms</pre> Der Parameter -T baut eine TCP-Verbindung auf, ohne einen http-Request an den Webserver der Zieladresse zu senden. Die Anfrage taucht daher nicht im Webserverlog des Zielservers auf. Im Beispiel sind neun Hops/Router involviert.

Neben den Prüfwerkzeugen auf Shell-Ebene besitzen die heutigen Netzwerkkomponenten oftmals einen integrierten Webserver, über welchen sie sich bedienen lassen.

Beispiel: Router

Das folgende Bild zeigt die grundsätzliche LAN-Konfiguration einer Fritz!Box. Die Weboberfläche ist über die IP-Adresse des Routers aufrufbar, in diesem Beispiel also über <http://192.168.178.1>:

Geben Sie die IPv4-Adresse an, unter der die FRITZ!Box im lokalen Netzwerk erreichbar ist.

Achtung!
Änderungen auf dieser Seite können dazu führen, dass die FRITZ!Box nicht mehr erreichbar ist. Beachten Sie unbedingt die Hilfe, bevor Sie Änderungen vornehmen.

Heimnetz

IPv4-Adresse: 192 . 168 . 178 . 1

Subnetzmaske: 255 . 255 . 255 . 0

☒ DHCP-Server aktivieren

DHCP-Server vergibt IPv4-Adressen

von: 192 . 168 . 178 . 20

bis: 192 . 168 . 178 . 200

Gültigkeit: 10 Tage

Die vergebenen IP-Adressen werden nach Ablauf der Gültigkeit wieder freigegeben.

Wenn Sie einen anderen DNS-Server in Ihrem Heimnetz verwenden möchten, tragen Sie hier dessen IP-Adresse ein, damit die FRITZ!Box diese den Geräten im Heimnetz bekannt gibt.

Lokaler DNS-Server: 192 . 168 . 178 . 56

In der Abbildung ist zu sehen, dass der IPv4-Adressbereich für das lokale Netzwerk (LAN) die 192.168.178.1/24 ist.

Wichtig: Dieser Adressbereich muss angepasst werden, wenn mehrere Standorte über VPN miteinander verbunden werden sollen. Die Standorte müssen unterschiedliche Adressbereiche nutzen.

Lokale Server sollten zudem stets mit einer statischen IP-Adresse arbeiten. Im Beispiel oben vergibt der Router lediglich IP-Adressen von 192.168.178.20 bis 192.168.178.200. Server in diesem Netzwerk können daher eine statische IP-Adresse ab 192.168.178.201 erhalten.

Ein lokaler DNS-Server ist üblicherweise der Router selbst, im Beispiel oben also die IP 192.168.178.1. Hier wurde ein separater DNS-Server im Netzwerk bereitgestellt.

LE 3 - Vorstellung des Virtualisierungskonzeptes im Leistungsportfolio

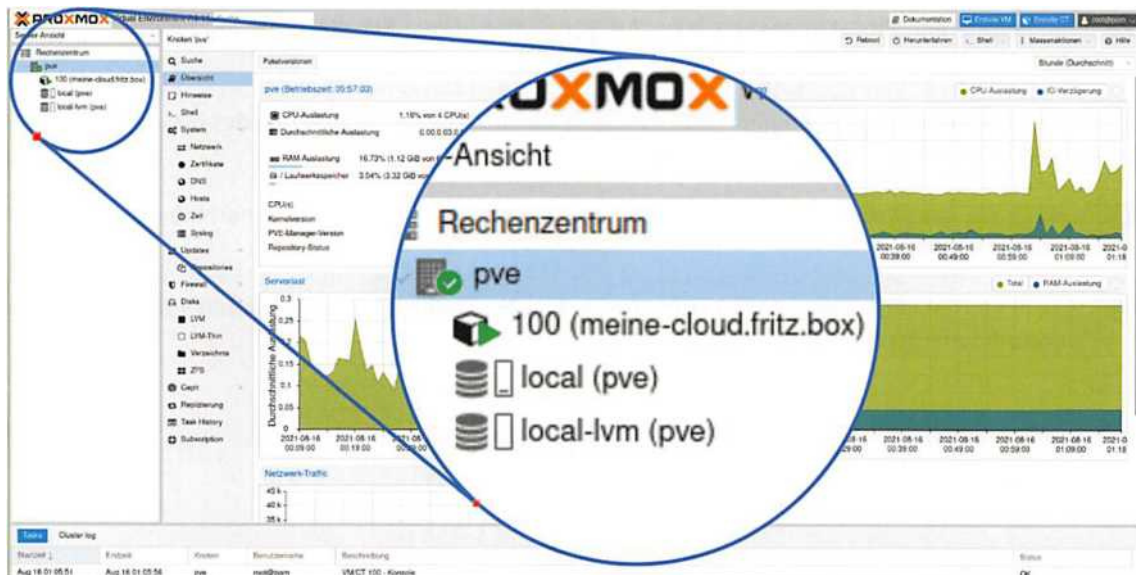
In diesem Abschnitt stellen die Auszubildenden der JIKU IT-Solutions ihrer Geschäftsführung das Virtualisierungskonzept vor, wie es den Kunden angeboten werden soll.

Vorab haben die Auszubildenden Virtualisierungsplattformen wie „Proxmox Virtual Environment“, „oVirt“, „Xen Cloud Panel Next Generation“ (XCP NG) und „OpenNebula“ evaluiert. Dabei haben sie folgende Erkenntnisse gewonnen:

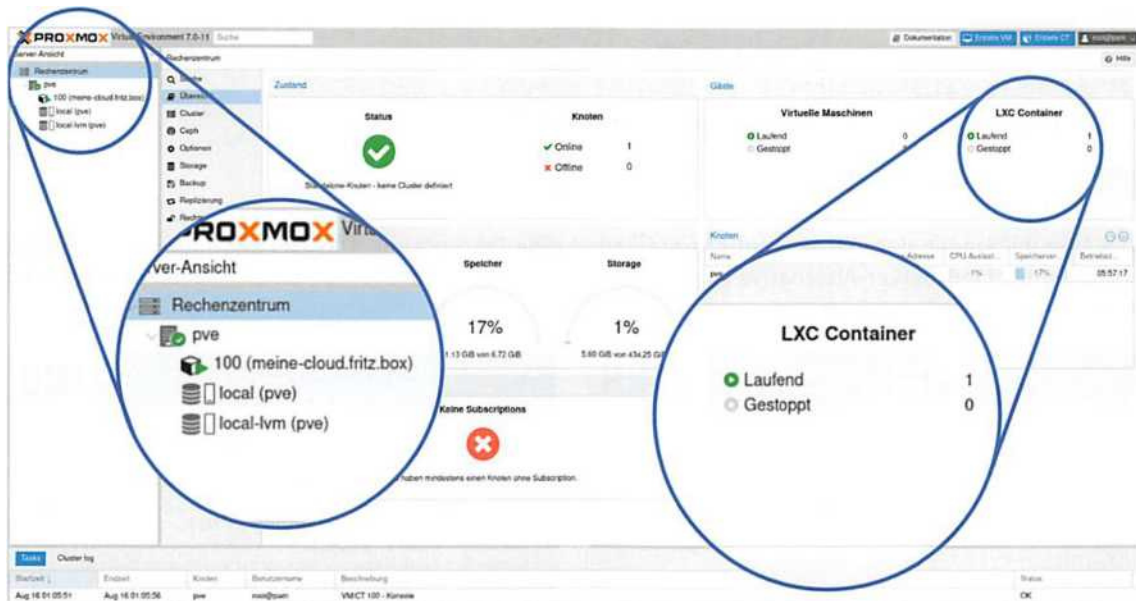


Potenziale von Virtualisierungsplattformen für IT-Dienstleister wie JIKU IT-Solutions	
Bedarfsgerechte Vermietung	Durch den Einsatz einer einheitlichen Virtualisierungsplattform auf allen Hardwareplattformen kann JIKU IT-Solutions eigene Ressourcen gezielt vermieten.
Einbindung von „Dritt“-Ressourcen	Aufgrund der Fähigkeit der Virtualisierungsplattformen, Bare-Metal-Server und virtuelle dedizierte Server als Knoten einzubinden, kann ein hybrides Rechenzentrum erstellt und vermietet werden.
Kunde hat die Wahl	Die Kunden von JIKU IT-Solutions können ihre eigenen Bare-Metal-Server durch JIKU IT-Solutions in die hybride Infrastruktur einbinden lassen (Managed Services bzw. Outsourcing aus Sicht des Kunden).

Aufgrund des Reifegrades und der geringen Einstiegshürden entscheiden sich die Auszubildenden der JIKU IT-Solutions für „Proxmox Virtual Environment“. Sie ist aus Unternehmenssicht für das Management hybrider IT-Infrastrukturen gut geeignet. Die folgende Abbildung zeigt die Weboberfläche der Plattform der JIKU IT-Solutions. Jede Serverhardware wird dabei als „Knoten“ dargestellt.

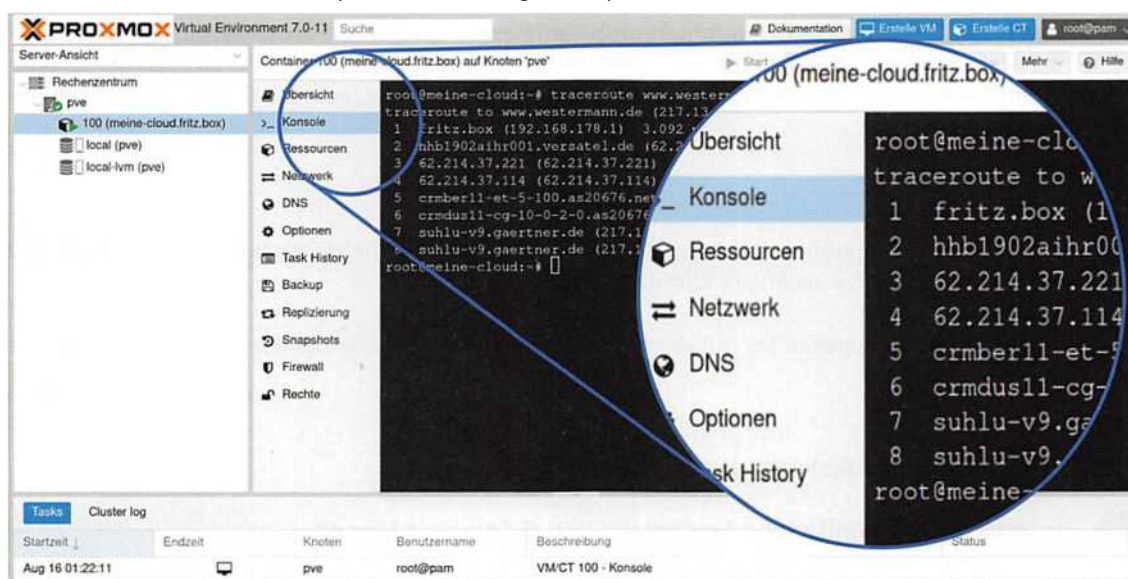


In der Abbildung hat JIKU IT-Solutions einen Knoten „pve“ eingerichtet. Auf diesem läuft ein Container mit der ID 100 und darin eine Nextcloud. Die Graphen auf der rechten Seite zeigen die Auslastung des pve-Knotens. CPU-Auslastung und Serverlast sind sehr gering. Weitere Vorteile sind ein einheitliches Monitoring auf Rechenzentrums-, Knoten- und VM-/Container-Ebene.



Weboberfläche der Virtualisierungsplattform zur Anzeige aller Knoten (Bare Metal)

Über die Weboberfläche der Virtualisierungsplattform können neben Snapshots und Back-ups auch weitere Linux-Container erstellt werden. Die Verbindung zur Shell des Servers lässt sich direkt im Browser herstellen (siehe Abbildung unten).



Die Shell wird direkt im Browser ausgeführt, Menüpunkt Konsolen.

Ziele der Informationsveranstaltung vorstellen

Die Auszubildenden der JIKU IT-Solutions erarbeiten eine Präsentation. Das Ziel der Präsentation ist die Vorstellung einer „Server-Alternative ohne Hardware vor Ort“. Dazu legen sie einen „Musterkunden“ fest. Dieser zeichnet sich wie folgt aus:

Ziele des Kunden

JIKU

Ein KMU mit 5 Mitarbeiter*innen möchte ihre 6 Jahre alte Serverhardware ersetzen.

- Lokaler Fileserver (4 Kerne, 24 GB Speicher, 4 TB NAS)
- Cloud-Laufwerke über OneDrive

2

Anwendungsfälle des Kunden

JIKU

Folgende Anwendungsfälle müssen überführt werden:

- CRM Software auf Microsoft SQL Datenbank inkl. Veranstaltungsmanagement
- VoIP in der Cloud, Anbindung an CRM über TAPI
- Videokonferenzen in der Cloud
- Homeoffice-Betrieb über Terminalserver und Remote Desktop
- Anmeldung und Rechteverwaltung über Active Directory
- E-Mails über Webhosting
- Kalender, Aufgaben über Outlook-Clients, lokales Office

3

Auch wenn in der Praxis die Kundenanforderungen variieren, so zeigt dieser Musterkunde die grundsätzlichen Herausforderungen vieler Kunden: alte Hardware, alte Zugriffskonzepte, hohe Lizenzkosten, hoher Pflegebedarf, großer Angriffsvektor wegen Einbindung von Homeoffices, keine IT-Fachkraft für die Administration etc.

Ein Virtualisierungskonzept erläutern

Für die Auszubildenden sieht das Zielszenario für Kunden der JIKU IT-Solutions wie folgt aus:

Zielszenario

JIKU

JIKU Virtualisierungskonzept

4

Virtualisierungskonzept von JIKU	
Idee	In dem Konzept mietet der Kunde einen virtuellen dedizierten Server bei JIKU IT-Solutions oder einem anderen Provider.
Installation	Das Einrichten der Virtualisierungsplattform sowie auf Wunsch die Wartung und Administration dieser Plattform übernimmt JIKU IT-Solutions. In der Abbildung stellt der Knoten 1 die Weboberfläche für JIKU IT-Solutions bereit.

Virtualisierungskonzept von JIKU	
Betrieb	Über die Weboberfläche erstellt JIKU IT-Solutions die virtuellen Maschinen, erstellt Back-ups, führt Updates und Upgrades durch, führt Roll-backs der Server durch, falls Updates bzw. Upgrades nicht funktionieren.
Erweiterbarkeit	Aufgrund der Fähigkeit des Kaskadierens kann in den VDS wiederum die Virtualisierungsplattform installiert werden. Die Verbindungen der Knoten untereinander laufen über ssh, der Administrator greift über https zu.
Ausfallsicherheit	Alle Knoten halten die Konfigurationen der anderen Knoten vor und synchronisieren sich. Fällt ein Knoten aus, haben die anderen weiterhin die Konfiguration inklusive der Weboberfläche. Der Administrator/DevOp loggt sich über einen anderen Knoten ein. Liegen die virtuellen Maschinen auf einem RAID, so kann ein anderer Knoten die VMs nachstarten.
Hochverfügbarkeit	Knoten können so konfiguriert werden, dass sie hoch verfügbar sind. In diesem Modus starten die übrigen Knoten selbstständig virtuelle Maschinen nach, wenn sie ausfallen.

Für den Musterkunden empfehlen die Auszubildenden das folgende Zielszenario. Anwendungen, die bereits als SaaS gemietet sind, verbleiben als SaaS, wenn der Kunde zufrieden damit ist. Anwendungen des lokalen Servers werden auf einen VDS verlagert.

Zielszenario	Anwendungsfälle zukünftig
Neue Serverhardware anmieten bei Provider des Vertrauens: • VDS mit mind. 6 Kernen, 24 GB Speicher, 4 TB • Virtualisierungsplattform „Proxmox“ einsetzen • „Nextcloud“ einrichten für Laufwerke, Kalender, Aufgaben, Zusammenarbeit • Zugriffe auf CRM und „Nextcloud“ erfolgen über Browser und Apps • Virtuelle Maschinen (VM) für Serveranwendungen	Die Anwendungsfälle werden wie folgt abgebildet: • Die Anwendungsfälle werden wie folgt abgebildet: • CRM-Software als Cloud-Lösung als virtuelle Maschine auf dem VDS • VoIP in der Cloud, Anbindung an CRM über TAPI • Videokonferenzen in der Cloud • Homeoffice-Betrieb über Terminalserver und Remote-Desktop • Anmeldung und Rechteverwaltung über Active Directory • E-Mails über Webhosting • Kalender, Aufgaben über Outlook-Clients, lokales Office

Managed Services - Leistungsstufen der Mitwirkung

Serveranwendungen werden in immer kürzeren zeitlichen Abständen von der Community und den Herstellern aktualisiert. Neben Fehlerbehebungen kommen auch neue Funktionen hinzu.

Gerade bei Serveranwendungen ist es zwingend erforderlich, diese bei Sicherheitsupdates und Fehlerbehebungen zeitnah zu aktualisieren. Für Kunden stellt sich daher die Frage, inwieweit sie bei Updates und Administration mitwirken möchten.

Folgende „Managed Services“ möchte JIKU IT-Solutions anbieten:

JIKU Managed Services	
Management der hybriden Infrastruktur	Hierunter fällt der Betrieb des gesamten Kundenrechenzentrums. Für diese Tätigkeiten sind DevOp-Skills erforderlich.

JIKU Managed Services	
Server-Management	Hierunter fallen das Einrichten von E-Mail-Accounts, das Update, Upgrade, Back-up und Rollback von Serveranwendungen, z. B. über „cPanel“ oder „Plesk“. Hierzu zählen ebenfalls das Erstellen von Snapshots und Back-ups und das Rollback virtueller Maschinen. Für diese Tätigkeiten sind Administrator-Skills erforderlich.
Anwendungsmanagement	Hierunter fallen die Administration der VoIP-Anlage, der Nextcloud-Anwendung, der CRM-Anwendung etc. Diese Anwendungen besitzen eine eigene webbasierte Administrationsoberfläche, die gezielt auf die Anwendung ausgerichtet ist. Für diese Tätigkeiten ist Know-how zur jeweiligen Anwendung erforderlich.

Die Abbildung zeigt die Servermanagement-Oberfläche „cPanel“ für den Nextcloud-Server der JIKU-BBS.



Die Serveranwendung Nextcloud mit der URL <https://cloud.jiku-bbs.de> lässt sich per Mausklick stagen, klonen und sichern.

Eine Staging-Umgebung ist eine Kopie der Serveranwendung. Auf dieser Kopie können Änderungen vorgenommen werden. Die Staging-Umgebung kann im Anschluss mit der ursprünglichen Umgebung per Mausklick zusammengeführt werden.

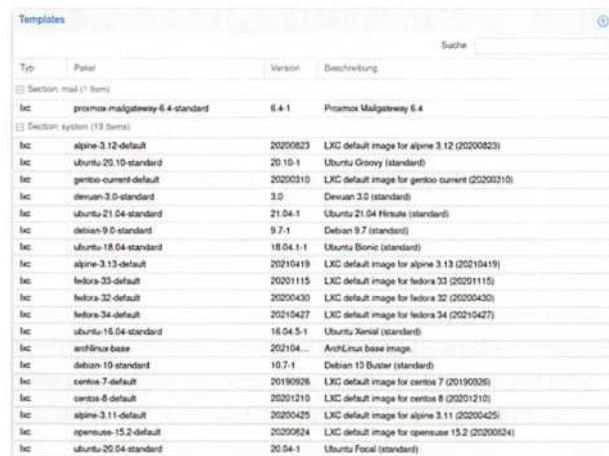
Kunden können entscheiden, welche Managed Services sie einkaufen möchten und welche sie selbst übernehmen wollen. Aufgrund der erforderlichen Skills und Know-hows ist darauf zu achten, dass sich der Kunde nicht „übernimmt“.

Leistungsstufen der Mitwirkung		
gering	mittel	hoch
Der Kunde möchte nur sehr gering mitwirken. Diese Kunden kaufen die Administration und das gesamte Management der Infrastruktur ein. Zu klären ist, welches Anwendungsmanagement der Kunde übernehmen möchte. Beispiele wären das Einrichten von Telefonen für neue Mitarbeiter, das Einrichten von Benutzerzugängen in den übrigen Anwendungen etc.	Der Kunde möchte gerne mitwirken. Es ist zu klären, welche administrativen Tätigkeiten er aus den Bereichen des Anwendungs- und/oder Servermanagements übernehmen möchte. Alle weiteren Leistungen bietet JIKU IT-Solutions als Managed Services an.	Der Kunde hat eine eigene IT-Abteilung. Diese übernimmt alle Administrationsbereiche selbst.

LE 4 - Ausblick geben: Marktplätze für Container und virtuelle Anwendungen

Der Komfort für das Management von virtuellen Servern wird durch das Einbinden von Marktplätzen noch einmal gesteigert. Durch solch eine Einbindung können in der Weboberfläche der Virtualisierungsplattformen sogenannte Vorlagen (Templates) für Server genutzt werden (siehe Abbildung rechts)

Die Abbildung zeigt bereits vorhandene Vorlagen auf dem Host der JIKU IT-Solutions, die in sogenannten LXC-Linux-Containern per Mausklick eingerichtet werden können. Linux-Container laufen in einer abgeschotteten Sandbox des Host-Betriebssystems und sind somit leichtgewichtiger als virtuelle Maschinen.



Typ	Palet	Version	Beschreibung
[+] Section: mail (1 items)			
lxc	proxmox-mailgateway 6.4-standard	6.4-1	Proxmox Mailgateway 6.4
[+] Section: system (19 items)			
lxc	alpine-3.12-default	20200823	LXC default image for alpine 3.12 (20200823)
lxc	ubuntu-20.10-standard	20.10-1	Ubuntu Groovy (standard)
lxc	gentoo-current-default	20200310	LXC default image for gentoo current (20200310)
lxc	devuan-3.0-standard	3.0	Devuan 3.0 (standard)
lxc	ubuntu-21.04-standard	21.04-1	Ubuntu 21.04 Hirsute (standard)
lxc	debian-9.0-standard	9.7-1	Debian 9.7 (standard)
lxc	ubuntu-18.04-standard	18.04.1-1	Ubuntu Bionic (standard)
lxc	alpine-3.13-default	20210419	LXC default image for alpine 3.13 (20210419)
lxc	fedora-33-default	20201115	LXC default image for fedora 33 (20201115)
lxc	fedora-32-default	20200430	LXC default image for fedora 32 (20200430)
lxc	fedora-34-default	20210427	LXC default image for fedora 34 (20210427)
lxc	ubuntu-16.04-standard	16.04.5-1	Ubuntu Xenial (standard)
lxc	archlinux-base	202104...	ArchLinux base image
lxc	debian-10-standard	10.7-1	Debian 10 Buster (standard)
lxc	centos-7-default	20190926	LXC default image for centos 7 (20190926)
lxc	centos-8-default	20201210	LXC default image for centos 8 (20201210)
lxc	alpine-3.11-default	20200425	LXC default image for alpine 3.11 (20200425)
lxc	openuse-15.2-default	20200624	LXC default image for openuse 15.2 (20200624)
lxc	ubuntu-20.04-standard	20.04-1	Ubuntu Focal (standard)

Vorlage (Template) auf dem Host der JIKU IT-Solutions

Die Einbindung von Marktplätzen vereinfacht die Installation neuer Container auf der eigenen Virtualisierungsplattform und somit auf dem eigenen Server bzw. beim Provider des Vertrauens. Wie bei jeder Software gilt auch bei den Marktplätzen, dass die Korrektheit und Authentizität der Container vor der Nutzung geprüft werden sollten. Folgende Marktplätze können bereits heute in Virtualisierungsplattformen, z. B. „Proxmox“ oder „OpenNebula“ genutzt werden:

Marktplätze für Container und virtuelle Anwendungen	
Marktplatz	Beschreibung
DockerHub	bietet auf https://hub.docker.com/search?q=&type=image eine Plattform mit verifizierten docker-Images
Linux Containers	bietet auf https://images.linuxcontainers.org/ öffentliche LXD/LXC Images mit „debian“, „AlmaLinux“, „OpenSuse“, „Ubuntu“ etc. an
Turnkey Linux	bietet auf https://www.turnkeylinux.org vorkonfigurierte Linux-Container an, z. B. „OpenVPN“, „Mattermost“, „Nextcloud“, „ProcessMaker“, „SuiteCRM“
Softaculous	kostenpflichtiger Marktplatz für Webanwendungen des LAMP Stacks; LAMP steht für Linux - Apache - MySQL - PHP; wird z. B. von „cPanel“ genutzt („cPanel“ selbst benötigt als Unterbau z. B. einen Ubuntu-Server)

Marktplatz	Beschreibung
Eigener Marktplatz	über einen eigenen Marktplatz können sich DevOps ihre eigenen Server-Vorlagen erstellen und wieder verwenden

Empfehlung der Auszubildenden der JIKU IT-Solutions

Bei allen Möglichkeiten, die sich aufgrund der Virtualisierung ergeben, empfehlen die Auszubildenden, für jeden Kunden vorab ein Proof-of-Concept-Projekt zu vereinbaren. Die Migration der einen oder anderen lokalen Serveranwendung sollte nur mit Unterstützung des Herstellers durchgeführt werden. Nur dieser weiß, wie beispielsweise eine Datenbank von MS SQL-Server auf MySQL durchgeführt wird. Parallel zu diesem Proof of Concept arbeiten die Mitarbeiter mit der „alten“ Infrastruktur. Nach dem Proof of Concept entscheidet der Kunde, wie die Umsetzung erfolgen soll.

TAG 15 - Vertiefung des Wissens und Modulprüfung

LE 1 - Einleitung

Der letzte Tag in diesem Modul bietet Ihnen die Möglichkeit der Wiederholung und Vertiefung Ihres Wissens. Sollten es noch offene, nicht vollständig bearbeitete Modul-Inhalte geben, nutzen Sie den heutigen Tag zur Komplettierung.

LE 2 - Modulprüfung

120 Minuten zu denen wir Ihnen recht viel Erfolg wünschen!