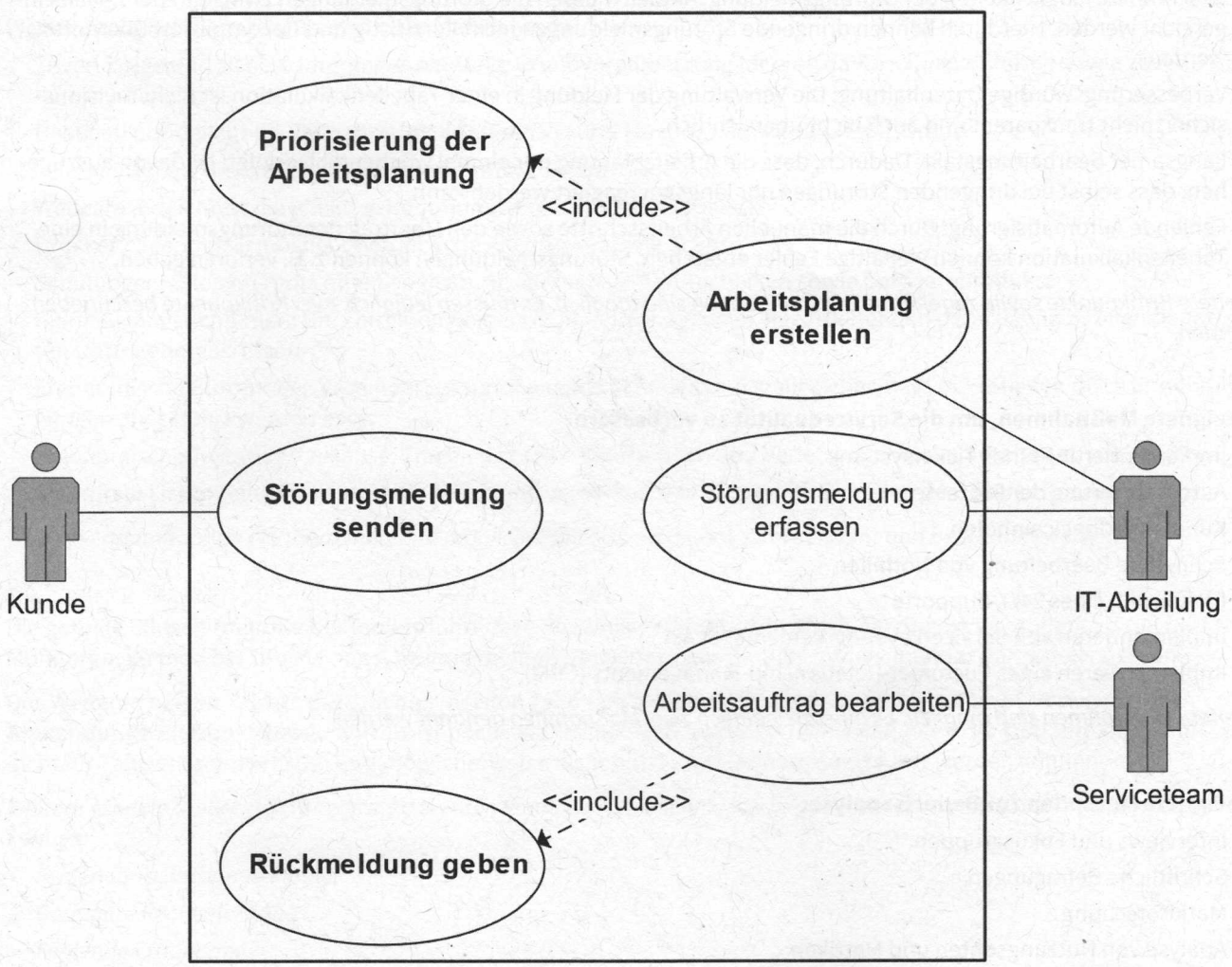
1. Aufgabe

a)



Weiterführende Informationen:

Ein Anwendungsfalldiagramm ist ein UML-Diagramm, welches verwendet wird, um die verschiedenen Interaktionen zwischen Akteuren (z. B. verschiedenen Rollen) und einem System oder einer Anwendung zu visualisieren. Es zeigt die möglichen Anwendungsfälle / Aktionen, die von den Akteuren ausgelöst werden können, und wie sie miteinander verknüpft sind.

Akteure werden außerhalb der Systemgrenzen (Kästchen, das alles umrahmt) dargestellt. Die Anwendungsfälle / Aktionen befinden sich innerhalb der Systemgrenzen und werden oval dargestellt.

Anwendungsfälle können auf unterschiedliche Arten miteinander verbunden werden:

Include-Assoziation (Einbeziehen): Ein Anwendungsfall beinhaltet immer einen weiteren Anwendungsfall

Extend-Assoziation (Erweitern): Ein Anwendungsfall kann durch einen weiteren Anwendungsfall erweitert werden.

In der vorliegenden Aufgabe wurde die Erweiterung der Anwendungsfälle stets mit „immer“ beschrieben, daher liegt hier eine Include-Assoziation vor.

d)

Vorteile von Homeoffice für die Beschäftigten	Nachteile von Homeoffice für die Beschäftigten
– Flexiblere Arbeitszeiten – Keine Fahrtkosten zur Arbeitsstelle – Keine Pendelzeiten – Weniger Stress durch Verkehr – Verbesserte Work-Life-Balance – Höhere Autonomie und Eigenverantwortung – Zugang zur eigenen Küche – Verbesserte Konzentration – Reduzierte Umweltauswirkungen durch weniger Pendeln – Erweiterte Auswahl an Arbeitsorten	– Soziale Isolation – Ablenkungen im häuslichen Arbeitsumfeld – Schwierigkeiten bei der Teamkommunikation – Vernachlässigung der Pausenzeiten – Technische Probleme – Risiken des Datenschutzes – Schwierigkeiten bei der Führung von Teams – Verlust von Büroausstattung und -ressourcen – Höhere Selbstdisziplin notwendig – Vermischung von Arbeits- und Privatleben – Berufliche Weiterbildung wird erschwert

Weitere Vor- bzw. Nachteile sind möglich. Es müssen lediglich zwei Vor- und zwei Nachteile genannt werden.

e)

Bereitschaftszeit:

20:00 Uhr – 06:00 Uhr → 10 Stunden

Kosten zur Abdeckung der Bereitschaftszeit:

(12,00 € + 15,00 € + 20,00 €) * 10 h = 470,00 €

Kosten der beanspruchten Anrufzeit:

(0,50 € * 150 Minuten) + (1,00 € * 100 Minuten) + (1,50 € * 50 Minuten) = 250,00 €

Gesamtkosten:

470,00 € + 250,00 € = 720,00 €

Gesamtzeit der Anrufe:

150 Minuten (First-Level) + 100 Minuten (Second-Level) + 50 Minuten (Third-Level) = 300 Minten

Einheitlicher Minutensatz:

720,00 € / 300 Minuten = 2,40 €

f)

Mögliche Argumente für eine E-Mail an Kunden:

- Die getrennte Abrechnung ermöglicht es Ihnen, genau zu wissen, wofür Sie bezahlen. Sie haben die volle Kontrolle über die Support-Kosten.
- Die Finanzierung der Hotline erfolgt nach dem Verursacherprinzip. Das heißt, dass Kunden, die die Hotline nicht in Anspruch nehmen, auch keine höheren Kosten erwarten müssen.
- Dadurch, dass die Hotline kostenpflichtig ist, können wir hochqualifizierte Mitarbeiter zur schnellstmöglichen Lösung Ihrer Anliegen beschäftigen.
- Das neue Zusatzangebot ist in der Kalkulation der Softwarekosten nicht enthalten und muss daher separat finanziert werden:

Weitere Lösungen sind möglich. Es müssen lediglich zwei Argumente formuliert werden.

3. Aufgabe

a)

Gesetzliche Regelungen zum Datenschutz in Deutschland:

- DSGVO (Datenschutz-Grundverordnung)
- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz (LDSG)
- Strafgesetzbuch (StGB)

Weiterführende Informationen:

Die Datenschutz-Grundverordnung **(DSGVO)** ist eine europäische Datenschutzverordnung, die am 25. Mai 2018 in Kraft getreten ist. Sie regelt den Schutz personenbezogener Daten von EU-Bürgern und ersetzt die früheren Datenschutzrichtlinien.

Das Bundesdatenschutzgesetz **(BDSG)** ist ein deutsches Gesetz, das den Datenschutz in Deutschland regelt. Es ergänzt die Datenschutz-Grundverordnung (DSGVO) und enthält spezifische nationale Regelungen für den Datenschutz.

Das Landesdatenschutzgesetz **(LDSG)** ist ein Datenschutzgesetz, das auf Landesebene in den einzelnen deutschen Bundesländern existiert. Jedes Bundesland kann sein eigenes LDSG erlassen, um spezifische Regelungen und Vorschriften für den Datenschutz innerhalb des jeweiligen Landes festzulegen. Das LDSG ergänzt sowohl die DSGVO als auch das BDSG.

Das Strafgesetzbuch **(StGB)** ist relevant für den Datenschutz in Deutschland, da es Straftatbestände im Zusammenhang mit Datenschutzverletzungen und dem Missbrauch von personenbezogenen Daten regelt (siehe z. B. § 202a StGB „Ausspähen von Daten" oder § 203 StGB „Verletzung von Privatgeheimnissen").

b)

Zugriffsschutz auf mobile Datenträger	Verschlüsselung der lokalen SSD
Zutrittsschutz Telearbeitsplatz	– Nutzung eines separaten sowie mit Sicherheitsschlössern/-türen gesicherten Arbeitsraums – Verstauen aller Arbeitsmittel zur Telearbeit in einem abschließbaren Schrank o. ä. – Beschränkter physischer Zugang durch individuelle Zugangsberechtigungen
Sichere Anmeldung am Laptop	– Verwenden einer biometrischen Authentifizierung (Fingerabdruck, Gesichtserkennung etc.) – Nutzen mehrerer Faktoren zur Authentifizierung und Anmeldung (Multi-Faktor-Authentifizierung) – Konfiguration zusätzlicher Sicherheitsfragen bei Anmeldung
Sichere Datenkommunikation	– Verwendung einer Public Key Infrastruktur (PKI) um die Integrität der Daten über Zertifikate zu prüfen – Implementierung von Firewalls und Intrusion Detection / Prevention Systemen – Durchgängig verschlüsselte Datenübertragung durch VPN-Nutzung
Transport von Datenträgern	– Durchgängige Beweiskette (Chain of Custody) zum Verlauf des Datenträgers pflegen – Verwenden von gesicherten Transportbehältern (Schutz vor physischen Schäden und äußeren Einflüssen) – Durchgängiges Tracking des Transports mittels GPS – Weitere Lösungen sind möglich. Es muss lediglich eine Maßnahme je Bereich angegeben werden.

ca)

Mögliche Kriterien für ein sicheres Passwort:

- Verwenden einer ausreichenden Passwortlänge (z. B. min. 12 Zeichen)
- Passwörter dürfen keinen persönlichen Bezug haben
- Verwendung von Sonderzeichen, Ziffern sowie Groß- und Kleinbuchstaben
- Sicherstellen, dass das Passwort oder Teile des Passwortes in keinem Wörterbuch zu finden sind
- Verwendung unterschiedlicher Passwörter für unterschiedliche Zugänge

Weitere Lösungen sind möglich. Es müssen lediglich zwei Kriterien genannt werden.

cb)

	Vorteil	**Nachteil**
In Cloud-Speicher hochladen	– Von überall aus zugänglich, sofern ein Zugang zum Internet besteht – Kein physischer Speicher vor Ort notwendig	– Cloud-Anbieter könnte kompromittiert werden – Cloud-Anbieter muss gesichert sein und gemäß der geltenden Datenschutzrichtlinien handeln
Auf USB-Stick speichern	– Zugriff auch ohne Internet und mobil möglich	– Kann leicht verloren gehen oder beschädigt werden
Wiederherstellungsschlüssel ausdrucken	– Keinerlei Nachverfolgbarkeit durch analoge Speicherung	– Gefahr, dass der Ausdruck mit der Zeit verblasst oder verloren geht – Aufbewahrung erfordert besondere Vertraulichkeit, da die Daten immer unverschlüsselt gedruckt werden

Weitere Lösungen sind möglich. Es muss lediglich jeweils ein Vor- und Nachteil genannt werden.

cc)

Vertraulichkeit:

Die Daten der SSD sind vor unbefugten Zugriffen geschützt. Selbst bei physischen Zugriffen auf die SSD, können die verschlüsselten Daten nur von befugten Personen gelesen werden.

Integrität:

Eine unbefugte Änderung oder Manipulation der Daten auf der SSD kann durch die Software erkannt werden.

cd)

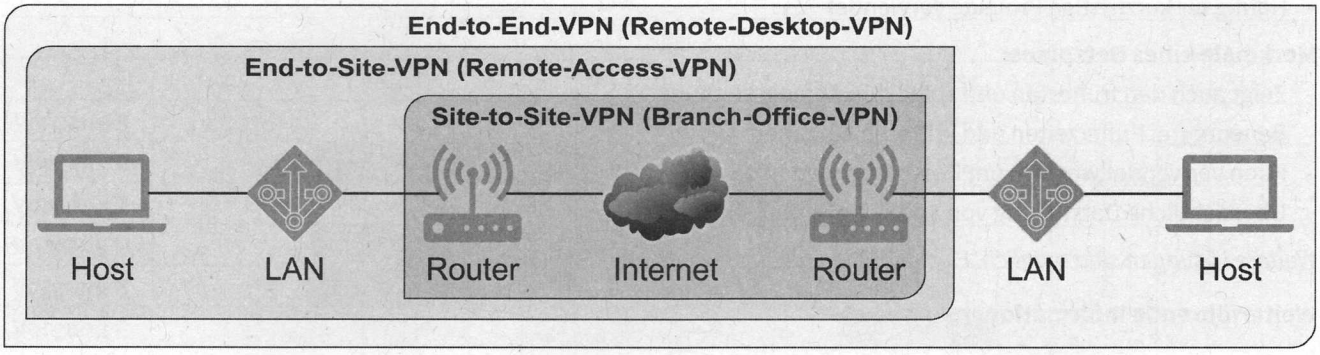
Durch die Verschlüsselung der Daten auf der SSD ist der direkte Zugriff auf die Daten unterbunden. Erst wenn das Passwort zum Entsperren des Datenträgers vorliegen würde, könnten die Daten vom Dieb eingesehen werden.

da)

Die Verwendung eines VPN bietet den Vorteil einer verschlüsselten Datenübertragung, sodass die Daten sicher zwischen dem Telearbeitsplatz und dem Firmennetzwerk übertragen werden können, selbst wenn eigentlich unsichere Netzwerke zur Datenübertragung genutzt werden.

Weiterführende Informationen:

Es gibt verschiedene Arten von VPN, die je nach Anwendungsfall genutzt werden. Im Kontext von Telearbeitsplätzen werden hauptsächlich End-to-Site- oder End-to-End-VPN verwendet.



Beispielhafte weitere sicherheitstechnische Vorteile eines VPN:

- Schutz vor Abhörversuchen wie z. B. Man-in-the-Middle-Angriffen
- Sichere Authentifizierung der Benutzer

db)

Die Identifizierung mithilfe des digitalen Zertifikats erfolgt durch eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA). Diese prüft die Identität des Antragstellers, erteilt ein Zertifikat und der Inhaber verwendet dieses Zertifikat zukünftig zur eindeutigen Identifizierung gegenüber dem Server im Firmennetz. Dies gewährleistet die Sicherheit und Vertrauenswürdigkeit der Identifizierung.

4. Aufgabe

aa)

Merkmale eines Gantt-Diagramms:

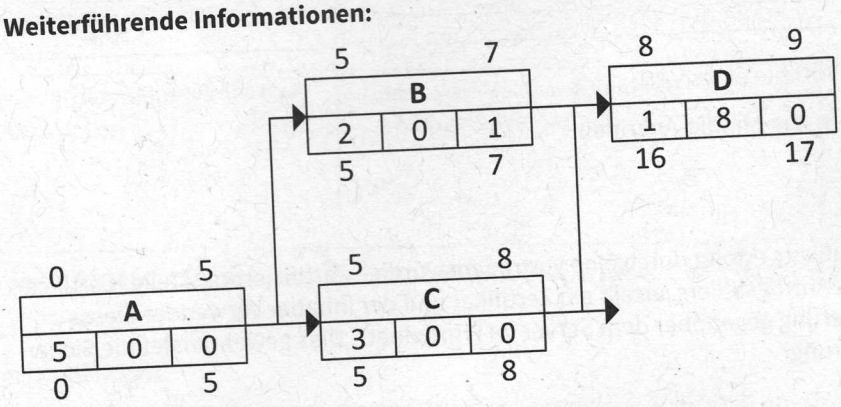
- Einfach zu verstehen und zu erstellen
- Erlaubt hinzufügen von Meilensteinen
- Zeigt Start- und Endtermine für Aufgaben
- Häufig für kurzfristige Projekte verwendet

Merkmale eines Netzplans:

- Zeigt auch den frühesten und spätesten Anfangszeitpunkt
- Benennt frei Pufferzeiten und kritische Aufgaben
- Kann verwendet werden, um Ressourcenbedarf zu planen
- Übersichtliche Darstellung von Abhängigkeiten der Projektphasen

Weitere Lösungen sind möglich. Es müssen lediglich je zwei Merkmale genannt werden.

Weiterführende Informationen:

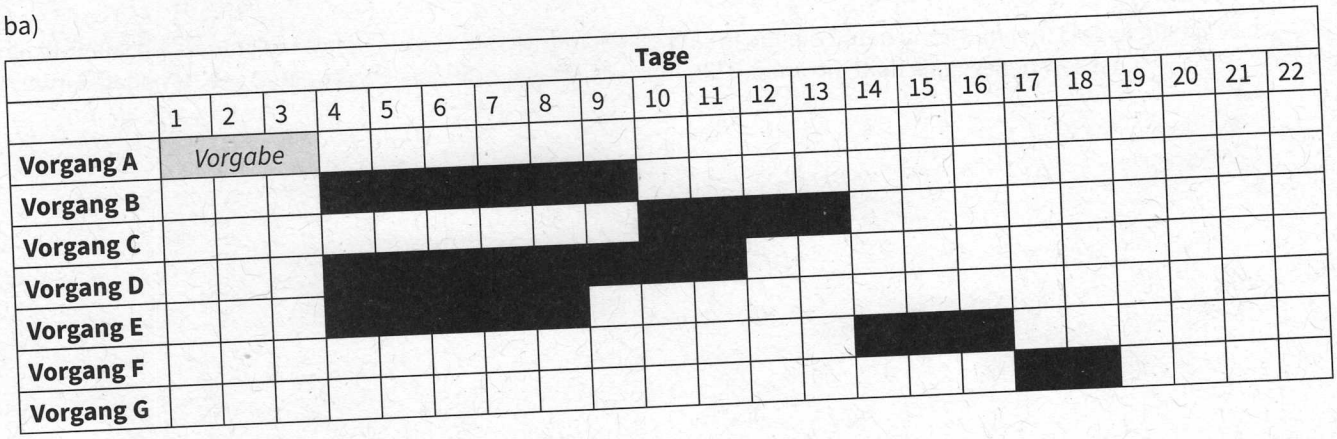


Ausschnitt eines Netzplans

ab)

Anforderungsanalyse	4	3	2	6	1	5

ba)



bb)

Das Projekt kann frühestens nach 18 Tagen beendet werden (siehe Ende Vorgang G).

bc)

Vorgang E

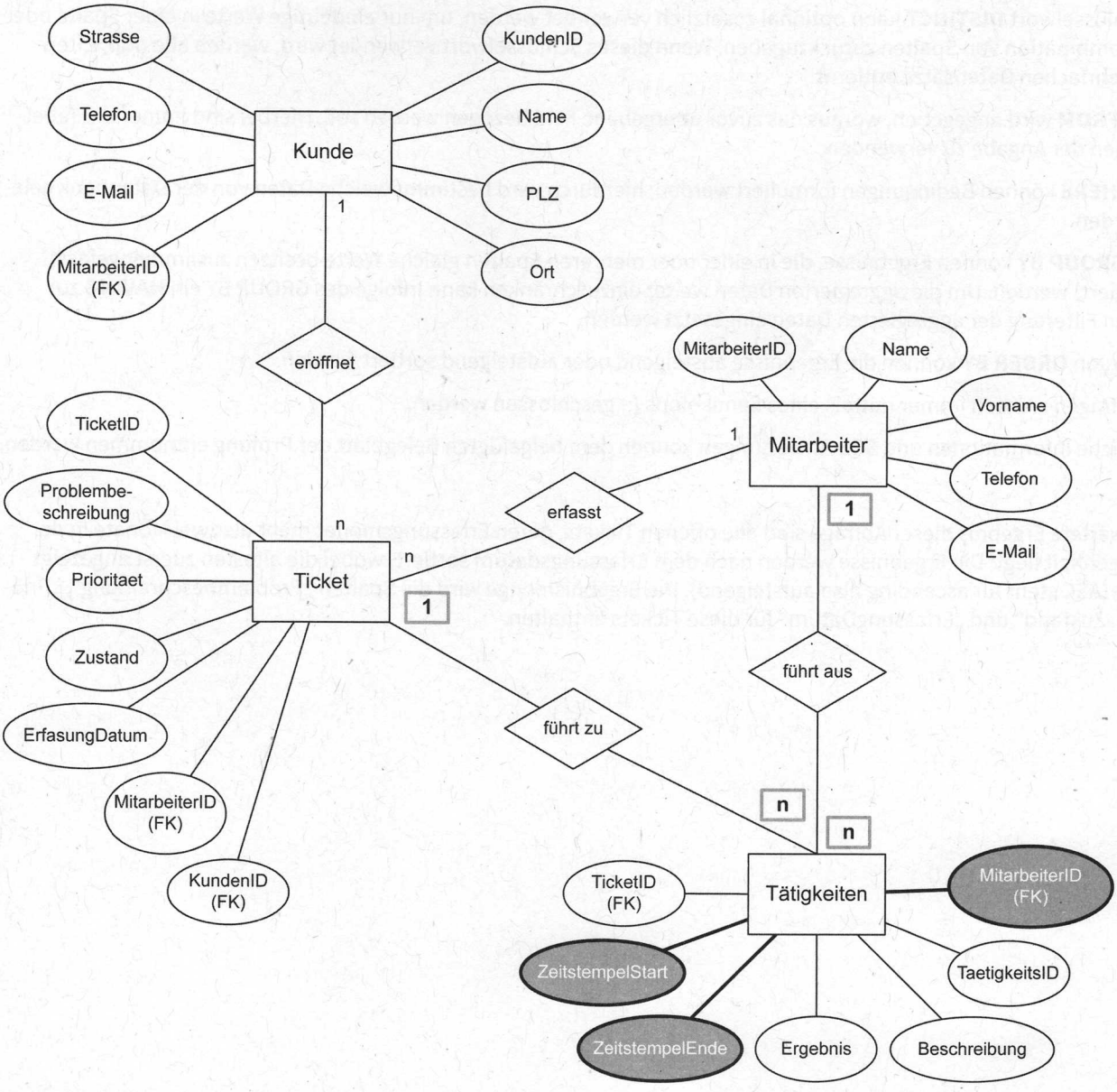
Weiterführende Informationen:

Pufferzeiten geben an, um welchen Zeitraum sich eine Tätigkeit verzögern darf, ohne dass sich der Abschluss des Gesamtprojektes verzögert.

Vorgang E kann sich um maximal 5 Tage nach hinten verschieben, ohne dass es zu einer Verzögerung im Gesamtprojekt kommt.

	Tage																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Vorgang A	*Vorgabe*																					
Vorgang B																						
Vorgang C																						
Vorgang D																						
Vorgang E									Pufferzeit													
Vorgang F																						
Vorgang G																						

ca)



cb)

```
SELECT Prioritaet, COUNT(TicketID) FROM Ticket GROUP BY Prioritaet;
```

cc)

```
SELECT COUNT(DISTINCT KundenID) AS AnzahlKunden FROM Ticket;
```

Weiterführende allgemeine Informationen zu SQL:

Bei SQL-Abfragen ist darauf zu achten, dass folgende Reihenfolge eingehalten wird:

1. SELECT ....
2. FROM ....
3. WHERE ... (optional)
4. GROUP BY ... (optional)
5. HAVING ... (optional)
6. ORDER BY ... (optional)

Durch das **SELECT** wird zunächst entschieden, welche Tabellenfelder bzw. -spalten ausgegeben werden sollen. Es sind hierbei zwingend die Spaltennamen der Angabe zu verwenden. Sollte im Rahmen der Ausgabe eine Umbenennung erforderlich sein, so hat diese über **AS *<Neuer Name>*** zu erfolgen.

Nach SELECT können außerdem verschiedene Funktionen verwendet werden (z. B. **MAX** zum Ermitteln des Maximalwertes, **SUM** zum Bilden einer Summe, **COUNT** zum Ermitteln der Anzahl der Datensätze oder **AVG** zur Ermittlung eines Durchschnittswertes).

Das Schlüsselwort **DISTINCT** kann optional zusätzlich verwendet werden, um nur eindeutige Werte in einer Spalte oder einer Kombination von Spalten zurückzugeben. Wenn dieses Schlüsselwort verwendet wird, werden alle doppelten oder mehrfachen Datensätze entfernt.

Mittels **FROM** wird angegeben, woraus das zuvor übergebene Feld bezogen werden soll. Hierbei sind immer die Tabellennamen der Angabe zu verwenden.

Über **WHERE** können Bedingungen formuliert werden, hierdurch wird bestimmt welche Daten von der Datenbank gelesen werden.

Durch **GROUP BY** können Ergebnisse, die in einer oder mehreren Spalten gleiche Werte besitzen zusammengefasst (aggregiert) werden. Um die aggregierten Daten weiter einzuschränken kann infolge des GROUP BY ein **HAVING** zur weiteren Filterung der aggregierten Daten eingesetzt werden.

Mithilfe von **ORDER BY** können die Ergebnisse absteigend oder aufsteigend sortiert werden.

SQL-Abfragen müssen immer mittels eines Semikolons (;) geschlossen werden.

Zusätzliche Informationen und SQL-Anweisungen können dem beigefügten Belegblatt der Prüfung entnommen werden.

cd)

Das erwartete Ergebnis dieser Abfrage sind alle offenen Tickets, deren Erfassungsmonat mehr als zwei Monate in der Vergangenheit liegt. Die Ergebnisse werden nach dem Erfassungsdatum sortiert, wobei die ältesten zuerst angezeigt werden (ASC steht für ascending also aufsteigend). Die Ergebnismenge wird die Spalten „Problembeschreibung“, „Prioritaet“, „Zustand“ und „ErfassungDatum“ für diese Tickets enthalten.