Arbeitsaufgaben in Abstimmung mit kundenspezifischen Geschäfts- und Leistungsprozessen

Machbarkeit von Projekten – AP1-Check

Die systematische Machbarkeitsanalyse bildet das Fundament jeder erfolgreichen Projektdurchführung im IT-Bereich. In der IT-Fachpraxis und speziell in der Prüfungssituation der Fachinformatiker-Abschlussprüfung ist die strukturierte Bewertung von Projekten nach klar definierten Dimensionen unerlässlich. Die zentrale Leitfrage lautet dabei: Können wir das Projekt technisch, organisatorisch, rechtlich und wirtschaftlich sauber liefern – mit vertretbarem Risiko?

Im Rahmen dieser Präsentation betrachten wir einen praxisnahen Mini-Fall: den vollständigen Austausch einer Firewall-Infrastruktur mit High-Availability-Konfiguration (HA), Integration kritischer Netzwerkdienste wie DHCP, DNS und Proxy, Implementierung erweiterter Security-Funktionen, umfassende Testszenarien sowie eine strukturierte Übergabe an den IT-Betrieb. Dieser Fall vereint alle wesentlichen Aspekte der Machbarkeitsanalyse und dient als roter Faden durch die verschiedenen Prüfungsdimensionen.

KERNKONZEPT

Machbarkeitsanalyse – die 5 Dimensionen

Die Machbarkeitsanalyse ist keine bloße Formalität, sondern ein systematisches Prüfverfahren, das alle kritischen Erfolgsfaktoren eines Projekts beleuchtet. In der Praxis und in Prüfungssituationen müssen Sie nachweisen können, dass Sie sämtliche Dimensionen strukturiert evaluieren und dokumentieren können.

Das Ergebnis einer vollständigen Machbarkeitsanalyse mündet stets in einer klaren, begründeten Entscheidung: **Go** (Projekt kann wie geplant durchgeführt werden), **Go mit Auflagen** (Projekt ist machbar, jedoch nur unter bestimmten Bedingungen oder mit Anpassungen) oder **No-Go** (Projekt sollte nicht durchgeführt werden, da Risiken zu hoch oder Machbarkeit nicht gegeben ist).

Technisch

Kompatibilität, Performance, Schnittstellen, erforderliche Skills und Tools vorhanden?

Wirtschaftlich

Lohnt sich das Projekt? Kosten-Nutzen-Verhältnis positiv? Budget gesichert?

Organisatorisch

Ressourcen, Termine und Abhängigkeiten realistisch planbar?

Rechtlich/Compliance

DSGVO-Konformität, Verträge, Lizenzen, Aufbewahrungspflichten geklärt?

Betrieblich

Betrieb, Monitoring, Backup, Updates und Support nachhaltig geregelt?

Arbeitsauftrag: Nennen Sie drei konkrete No-Go-Kriterien im Firewall-Fall – jeweils eines aus den Bereichen technisch, organisatorisch und rechtlich. Begründen Sie, warum diese Kriterien zum Projektabbruch führen würden.

Machbarkeitsanalyse – typische Prüfpunkte am Firewall-Beispiel

Die theoretischen Dimensionen der Machbarkeit müssen in der Praxis auf konkrete, prüfbare Kriterien heruntergebrochen werden. Nur so lässt sich eine objektive Bewertung vornehmen und ein fundiertes Go/No-Go-Statement erstellen. Im Firewall-Projekt ergeben sich spezifische technische und organisatorische Anforderungen, die systematisch abgearbeitet werden müssen.

Netzwerk-Kompatibilität

Prüfung: Passen die WAN/LAN-Interfaces der neuen Firewall zum bestehenden Netzwerkdesign? Sind VLAN-Konfigurationen, Routing-Protokolle und IP-Adressbereiche kompatibel? Müssen Switches oder Router angepasst werden?

High-Availability-Setup

Evaluierung: Ist die aktive/passive Verkabelung korrekt geplant? Funktioniert der Heartbeat-Mechanismus zuverlässig? Liegt die Failover-Zeit im akzeptablen Bereich (typisch unter 3 Sekunden)? Gibt es Single Points of Failure in der HA-Architektur?

Performance-Dimensionierung

Analyse: Security-Funktionen wie Deep Packet Inspection (DPI) und Intrusion Prevention System (IPS) sind CPU-intensiv. Reicht der Durchsatz der Firewall auch unter Last? Wurden Performance-Tests mit realistischen Traffic-Szenarien durchgeführt?

Wartung & Rollback

Planung: Sind Wartungsfenster mit allen Stakeholdern abgestimmt? Existiert ein detaillierter Rollback-Plan für den Fall von kritischen Fehlern? Wie lange dauert eine vollständige Rückkehr zum Ausgangszustand?

Dokumentation & Übergabe

Sicherstellung: Ist die Dokumentation so aufgebaut, dass der IT-Betrieb die Firewall später eigenständig administrieren, troubleshooten und warten kann? Wurden Schulungen für das Betriebspersonal eingeplant?

Arbeitsauftrag: Formulieren Sie fünf konkrete Prüfungsfragen, die Sie dem Kunden während der Machbarkeitsanalyse stellen würden. Achten Sie darauf, dass die Fragen spezifisch, messbar und relevant für die Go/No-Go-Entscheidung sind.

Stakeholderanalyse – wer kann das Projekt beeinflussen?

Stakeholder sind alle Personen, Gruppen oder Organisationen, die entweder **Einfluss auf das Projekt** haben oder **von dessen Ergebnissen betroffen** sind. Eine systematische Stakeholderanalyse ist entscheidend, um Erwartungen frühzeitig zu klären, potenzielle Widerstände zu identifizieren und eine zielgerichtete Kommunikationsstrategie zu entwickeln.

Schnellmatrix für AP1: Einfluss × Interesse

- **Hoch/Hoch:** Eng managen und kontinuierlich einbinden (z. B. IT-Leitung, Netzwerkadministratoren)
- **Hoch/Niedrig:** Zufrieden halten durch regelmäßige Statusupdates (z. B. Geschäftsführung)
- **Niedrig/Hoch:** Informieren über Fortschritte und Änderungen (z. B. Helpdesk-Team)
- **Niedrig/Niedrig:** Beobachten, keine aktive Kommunikation erforderlich

Stakeholder im Firewall-Projekt

Typische Stakeholder umfassen IT-Leitung, Netzwerkadministratoren, Security-Verantwortliche, Datenschutzbeauftragte, betroffene Enduser (bei möglichen Ausfällen), externe Dienstleister und Provider sowie gegebenenfalls Betriebsrat bei größeren organisatorischen Änderungen.

Arbeitsauftrag: Listen Sie sechs relevante Stakeholder für das Firewall-Projekt auf und ordnen Sie diese in die Einfluss/Interesse-Matrix ein. Begründen Sie Ihre Einordnung mit konkreten Beispielen.

Risikoanalyse – systematische Steuerung statt Bauchgefühl

Risikomanagement bedeutet nicht, Ängste zu schüren, sondern Unwägbarkeiten strukturiert zu identifizieren, zu bewerten und durch geeignete Maßnahmen zu steuern. Die Grundformel der Risikobewertung lautet: **Risiko = Eintrittswahrscheinlichkeit × Auswirkung**. Das Ergebnis ist eine priorisierte Risikoliste mit konkreten Maßnahmen nach den vier Strategien: vermeiden, vermindern, übertragen oder akzeptieren.

1

Interface-Fehlkonfiguration

Ursache: Falsche VLAN-Zuordnung oder IP-Konfiguration. **Auswirkung:** Gesamter Standort offline, kritischer Geschäftsstillstand. **Maßnahme:** Detaillierter Pre-Check, Test in isolierter Umgebung, schrittweise Migration. **Owner:** Netzwerkadministrator.

2

Performance-Einbruch durch Security-Features

Ursache: IPS/DPI aktiviert ohne ausreichende Dimensionierung. **Auswirkung:** Drastischer Durchsatzrückgang, Produktivitätsverlust. **Maßnahme:** Load-Tests vor Produktivschaltung, stufenweise Aktivierung von Features. **Owner:** Security-Verantwortlicher.

3

HA-Failover-Versagen

Ursache: Heartbeat-Konfiguration fehlerhaft, Netzwerklatenzen. **Auswirkung:** Single Point of Failure trotz HA-Investment. **Maßnahme:** Umfassende Failover-Tests unter Last, Monitoring der Heartbeat-Verbindung. **Owner:** IT-Leitung.

4

Wartungsfenster zu kurz

Ursache: Zeitplanung zu optimistisch, unvorhergesehene Probleme. **Auswirkung:** Projektabbruch ohne vollständigen Rollback, System in inkonsistentem Zustand. **Maßnahme:** Zeitpuffer einplanen, Rollback-Szenarien testen. **Owner:** Projektleiter.

5

Unzureichende Dokumentation

Ursache: Zeitdruck, fehlende Standards. **Auswirkung:** IT-Betrieb kann System nicht eigenständig administrieren, Wissensabhängigkeit. **Maßnahme:** Dokumentation als Projektmeilenstein definieren, Review durch Betriebsteam. **Owner:** Projektleiter.

Arbeitsauftrag: Erstellen Sie vier weitere Risiken für das Firewall-Projekt mit folgender Struktur: Ursache, Auswirkung, konkrete Maßnahme und verantwortlicher Owner. Bewerten Sie zusätzlich Eintrittswahrscheinlichkeit und Auswirkung auf einer Skala von 1-5.

PRÜFUNGSWISSEN

Risiko-Matrix – einfach und prüfungsnah

Bewertungssystem

Die Risiko-Matrix ist ein pragmatisches Werkzeug zur Visualisierung und Priorisierung von Projektrisiken. Sie kombiniert zwei Dimensionen:

- **Wahrscheinlichkeit (W):** niedrig / mittel / hoch
- **Auswirkung (A):** niedrig / mittel / hoch

Die Kombination beider Faktoren ergibt die Gesamtbewertung:

- **Rot:** Kritisches Risiko – sofort behandeln, eskalieren wenn nötig
- **Gelb:** Mittleres Risiko – Maßnahmen planen und monitoren
- **Grün:** Geringes Risiko – beobachten, keine aktive Maßnahme erforderlich

Prüfungsformulierung

In der AP1-Prüfung wird erwartet, dass Sie strukturiert argumentieren: *„Wir reduzieren Risiko X durch Maßnahme Y; das verbleibende Rest-Risiko wird akzeptiert, weil Z (Begründung: zu geringe Wahrscheinlichkeit / zu geringer Impact / Maßnahme unverhältnismäßig teuer)."*

Die visuelle Darstellung in der Matrix ermöglicht eine schnelle Priorisierung und hilft bei der Ressourcenallokation. Risiken im roten Bereich erfordern unmittelbare Aufmerksamkeit und verbindliche Maßnahmenpläne mit klaren Verantwortlichkeiten und Deadlines.

Stamm- und Bewegungsdaten – saubere Unterscheidung

Die präzise Unterscheidung zwischen Stamm- und Bewegungsdaten ist fundamental für Datenmodellierung, Datenschutz-Folgenabschätzungen und die Konzeption von Archivierungs- sowie Löschkonzepten. Diese Differenzierung wird in AP1-Prüfungen regelmäßig abgefragt und ist in der Praxis für DSGVO-Compliance unerlässlich.

Stammdaten

Stammdaten sind **relativ stabil** und beschreiben Grundobjekte oder Entitäten im System. Sie ändern sich selten und bilden die Basis für Geschäftsprozesse.

Typische Beispiele:

- Kundenstammdaten (Name, Adresse, Vertragsnummer)
- Artikelstamm (Produktbezeichnung, EAN, Kategorie)
- Mitarbeiterstamm (Personalnummer, Position, Abteilung)
- Server-Inventar (Hostname, IP, Hardwarespezifikationen)
- Benutzerkonten (Username, Rollen, Berechtigungen)
- Kostenstellen und Organisationseinheiten

Firewall-Projekt – Stammdaten

- Geräteinventar (Modell, Seriennummer, Standort)
- IP-Adressplan und Subnetz-Struktur
- Rollen- und Rechtekonzept
- Standort- und Kontaktdaten

Bewegungsdaten

Bewegungsdaten entstehen durch **operative Vorgänge** und ändern sich kontinuierlich. Sie dokumentieren Transaktionen, Events und zeitpunktbezogene Informationen.

Typische Beispiele:

- Bestellungen und Verkäufe (Datum, Menge, Betrag)
- Rechnungen und Zahlungsvorgänge
- Login-Events und Zugriffsprotokolle
- Tickets und Störungsmeldungen
- Sensor-Messwerte und Monitoring-Daten
- Lagerbewegungen (Ein-/Auslagerung)

Firewall-Projekt – Bewegungsdaten

- Traffic-Logs (Quelle, Ziel, Protokoll, Zeitstempel)
- IDS/IPS-Alerts und Security-Events
- Ticket-Historie für Changes und Incidents
- Change-Requests mit Genehmigungen
- Konfigurationsänderungen mit Audit-Trail

Arbeitsauftrag: Geben Sie fünf weitere Beispiele für Stamm- versus Bewegungsdaten aus einem typischen IT-Betrieb an. Erläutern Sie jeweils, warum die Klassifizierung korrekt ist.

Datenschutz & Informationssicherheit – AP1-Kernwissen

Die Themen Datenschutz und Informationssicherheit sind zentrale Säulen jeder IT-Projektplanung und werden in der Abschlussprüfung intensiv geprüft. Während Datenschutz sich auf den Schutz personenbezogener Daten konzentriert (rechtlicher Fokus, DSGVO), zielt Informationssicherheit auf den Schutz aller Informationswerte ab (technisch-organisatorischer Fokus, Schutzziele).

Datenschutz (DSGVO)

Kernfragen für jedes Projekt:

- Liegt Personenbezug vor? (direkt/indirekt identifizierbar?)
- Welcher Zweck rechtfertigt die Verarbeitung?
- Welche Rechtsgrundlage gilt? (Art. 6 DSGVO)
- Ist Datenminimierung umgesetzt?
- Existiert ein Löschkonzept?
- Wurde eine Datenschutz-Folgenabschätzung durchgeführt?
- Bei externen Dienstleistern: AVV (Auftragsverarbeitungsvertrag) geschlossen?

Firewall-spezifisch: Traffic-Logs und IPS-Alerts enthalten regelmäßig personenbezogene Daten (IP-Adressen, Usernamen, Zeitstempel). Diese müssen zweckgebunden verarbeitet, geschützt und nach festgelegter Retention-Period gelöscht werden.

Informationssicherheit

Schutzziele (CIA-Triade):

- **Vertraulichkeit (Confidentiality):** Nur Berechtigte erhalten Zugriff
- **Integrität (Integrity):** Daten sind korrekt und unverfälscht
- **Verfügbarkeit (Availability):** System ist im benötigten Zeitraum nutzbar

Typische Maßnahmen:

- Rechtekonzept nach Least-Privilege-Prinzip
- Verschlüsselung (Transport/Speicher)
- Patch-Management und Härtung
- Security-Monitoring und SIEM-Integration
- Backup-Strategie (3-2-1-Regel)
- Incident-Response-Plan

Firewall-spezifisch: Admin-Zugänge mit MFA, getrennte privilegierte Konten, Audit-Logging aller Konfigurationsänderungen, Update-/Firmware-Plan mit Test-Umgebung, Notfallzugang bei HA-Ausfall, tägliches Backup der Konfiguration mit Offsite-Speicherung.

Arbeitsauftrag: Nennen Sie sechs konkrete Maßnahmen passend zum Firewall-Projekt: drei aus dem Bereich Datenschutz und drei aus dem Bereich Informationssicherheit. Ordnen Sie jede Maßnahme einem Schutzziel zu.

BETRIEBSWIRTSCHAFT

Betriebswirtschaftliche Kennzahlen – AP1-Glossar

Betriebswirtschaftliches Grundverständnis ist essentiell für IT-Projekte und wird in der Prüfung regelmäßig abgefragt. Die folgenden Kennzahlen bilden das Fundament für Wirtschaftlichkeitsbetrachtungen und Go/No-Go-Entscheidungen.

1

Umsatz

Alle Erlöse aus Verkäufen oder erbrachten Dienstleistungen in einem bestimmten Zeitraum – **vor Abzug von Kosten**. Der Umsatz ist die „Topline" in der Gewinn- und Verlustrechnung und gibt an, wie viel ein Unternehmen oder Projekt einnimmt.

2

Gewinn

Das Ergebnis nach Abzug **aller Kosten** vom Umsatz. In vereinfachter Form: **Gewinn = Umsatz – Gesamtkosten**. Der Gewinn ist die „Bottomline" und zeigt die tatsächliche finanzielle Performance.

3

Deckungsbeitrag (DB)

Der Betrag, der nach Abzug der **variablen Kosten** vom Umsatz übrig bleibt: **DB = Umsatz – variable Kosten**. Der Deckungsbeitrag dient zur Deckung der Fixkosten; was danach übrig bleibt, ist der Gewinn. Prüfungsfalle: DB ≠ Gewinn!

4

Variable Kosten

Kosten, die direkt mit der Leistungserstellung schwanken (z. B. Materialkosten, Lizenzen pro Projekt, Fremdleistungen). Im IT-Projekt: Software-Lizenzen, externe Berater, Hardware-Beschaffung.

5

Fixkosten

Kosten, die unabhängig vom Leistungsvolumen anfallen (z. B. Miete, Gehälter, Abschreibungen). Im IT-Projekt: Anteil der Gehälter interner Mitarbeiter, Infrastruktur-Grundkosten, Raumkosten.

Praxisbeispiel: IT-Dienstleistungsprojekt

Ausgangssituation:

- Projektpreis (Umsatz): **8.000 €**
- Variable Kosten: **2.500 €**
  - Firewall-Lizenzen: 1.200 €
  - Externe Berater: 1.000 €
  - Kleinmaterial: 300 €

Berechnung Deckungsbeitrag:

DB = 8.000 € – 2.500 € = 5.500 €

Von diesem Deckungsbeitrag müssen noch die Fixkosten (anteilige Gehälter, Infrastruktur) gedeckt werden. Angenommen, der Fixkostenanteil für die Projektlaufzeit beträgt 3.500 €:

Gewinn = DB – Fixkosten = 5.500 € – 3.500 € = 2.000 €

Das Projekt trägt also 2.000 € zum Unternehmensgewinn bei.

Arbeitsauftrag: Berechnen Sie den Deckungsbeitrag für ein Projekt mit einem Preis von 12.000 € und variablen Kosten von 4.800 €. Nennen Sie zusätzlich zwei konkrete Beispiele für variable und zwei für fixe Kosten in einem typischen IT-Projekt.

ENTSCHEIDUNGSVORLAGE

Go/No-Go-Empfehlung – strukturierte Zusammenfassung

Die finale Entscheidungsvorlage fasst alle Analyseergebnisse kompakt zusammen und mündet in eine klare, begründete Empfehlung. Diese Struktur entspricht den Erwartungen in der AP1-Prüfung und ist auch in der Praxis das Standardformat für Projektfreigaben.

01

Ziel & Nutzen

Austausch der bestehenden Firewall-Infrastruktur durch eine moderne, hochverfügbare Lösung mit erweitertem Security-Feature-Set (DPI, IPS). Ziel: Erhöhung der Netzwerksicherheit, Reduktion von Ausfallzeiten durch HA-Konfiguration, Compliance mit aktuellen Security-Standards.

02

Machbarkeit (Ampel-Status)

- **Technisch:** GRÜN – Hardware kompatibel, Performance ausreichend dimensioniert, Know-how vorhanden
- **Organisatorisch:** GELB – Wartungsfenster knapp, erfordert präzise Planung und Zeitpuffer
- **Rechtlich:** GRÜN – DSGVO-Konformität durch Log-Management und AVV sichergestellt
- **Betrieblich:** GRÜN – Monitoring und Backup-Konzept vorhanden, Schulungen eingeplant

03

Top-3 Risiken + Maßnahmen

1. **Interface-Fehlkonfiguration (W: mittel / A: hoch):** Detaillierter Pre-Check, stufenweise Migration mit Tests
2. **Performance-Einbruch durch IPS (W: mittel / A: mittel):** Load-Tests vor Produktivschaltung, stufenweise Feature-Aktivierung
3. **HA-Failover-Versagen (W: niedrig / A: hoch):** Umfassende Failover-Tests, kontinuierliches Heartbeat-Monitoring

04

Wirtschaftlichkeit

Projektpreis: 18.500 €, variable Kosten: 6.200 € → **Deckungsbeitrag: 12.300 €**. Nach Abzug der Fixkosten (geschätzt 7.500 €) ergibt sich ein projektbezogener Gewinnbeitrag von ca. 4.800 €. Langfristig: Reduktion von Ausfallkosten und Security-Incidents, ROI innerhalb von 18 Monaten erwartet.

05

Entscheidung: GO mit Auflagen

Empfehlung: Projektfreigabe unter folgenden Bedingungen: (1) Erweitertes Wartungsfenster mit Zeitpuffer, (2) Verpflichtender Failover-Test in Test-Umgebung vor Go-Live, (3) Stufenweise Aktivierung der Security-Features mit Performance-Monitoring. Bei Einhaltung dieser Auflagen ist das Projekt mit vertretbarem Risiko durchführbar.

Arbeitsauftrag: Schreiben Sie eine eigene Go/No-Go-Empfehlung in fünf kompakten Bulletpoints für den beschriebenen Firewall-Fall. Berücksichtigen Sie alle fünf Dimensionen der Machbarkeit und begründen Sie Ihre Entscheidung nachvollziehbar.