Beschreibe die drei A's (Authentifizierung – Authentisierung – Autorisierung)

Diese drei Begriffe sind eng miteinander zusammenhängend und werden häufig verwechselt.

Authentisierung – das Nachweisen einer Identität

Im Rahmen einer Authentisierung erbringt eine Person einen Beweis dafür, dass sie ist, wer sie zu sein vorgibt. Im Alltag geschieht dies z. B. durch die Vorlage des Personalausweises. In der IT wird hierfür häufig ein Passwort in Kombination mit einem Benutzernamen genutzt.

Authentifizierung – die Prüfung des o. g. Identitätsnachweises auf seine Authentizität

Im Alltag geschieht dies z.B. durch die Prüfung des Personalausweis auf Urkundenfälschung und durch den Abgleich mit der Person. In der IT wird z.B. überprüft, ob die Kombination von Benutzernamen und Passwort im System existiert.

Autorisierung – das Gewähren des Zugangs zu den Privilegien, welche der erfolgreich nachgewiesenen Identität zustehen

Im Alltag kann dies nach Vorlage des Personalausweises der Zugang zu einem Unternehmen sein, bei dem man als Gast angemeldet wurde. Aber: Vielleicht erhält man als Gast nur den Zugang zum Besprechungsraum, nicht aber zur Montagehalle. In der IT kann nach der Autorisierung in einem Benutzerkonto z.B. gearbeitet werden. Aber wenn dieses Konto nicht über Administratorenrechte verfügt, können z.B. keine neuen Programme installiert werden.

Kurzgesagt: **Authentisierung** ist, wer du bist. **Authentifizierung** ist, nachzuweisen, wer du bist. **Autorisierung** ist, was du tun darfst, nachdem du bewiesen hast, wer du bist.

Löschpflichtige und aufzubewahrende Daten, welche Daten sind es nach Datenschutzgesetz

Wichtig ist, dass auch eine rechtmässig erfolgte Datenerhebung und -verarbeitung nicht unbegrenzt gespeichert und aufbewahrt werden darf, sondern strenge inhaltliche und vor allem zeitliche Grenzen gelten.

Die Datenspeicherung ist gemäss Art. 5 DSGVO nur so lange zulässig, wie es für den vorher festgelegten, eindeutigen sowie legitimen Zweck erforderlich und angemessen ist (Grundsatz der Speicherbegrenzung und Datenminimierung). Entfällt der Zweck, besteht nach Art. 17 DSGVO die Verpflichtung des datenschutzrechtlich Verantwortlichen – in dem Fall der Arbeitgeber – zur Löschung des Datensatzes.

Eine wichtige Ausnahme von der Löschpflicht besteht jedoch, wenn die weitere Verarbeitung und Speicherung der Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 17 Abs. 3b).

Grundsätzlich gilt hierbei: Spezialgesetzliche Aufbewahrungsfristen gehen stets den datenschutzrechtlichen Löschpflichten vor. Dementsprechend dürfen personenbezogene Daten nicht gelöscht werden, sofern derartige Aufbewahrungsfristen bestehen.

Datenschutz technische Fragen

Zugang zu den Daten

- Sicherheit der Räumlichkeiten
- Sicherheit der Serverräume
- Sicherheit des Arbeitsplatzes
- Identifizierung und Authentifizierung
- Zugang zu den Daten
- Zugang von ausserhalb der Organisation

Lebenszyklus von Daten

- Datenerfassung
- Protokollierung
- Pseudonymisierung und Anonymisierung
- Verschlüsselung
- Sicherheit der Datenträger
- Datensicherung
- Datenvernichtung
- Auslagerung von Arbeiten (Bearbeitung durch Dritte)
- Sicherheit und Schutz

Datenaustausch

- Netzsicherheit
- Verschlüsselung von Mitteilungen
- Unterzeichnen von Mitteilungen
- Übergabe von Datenträgern
- Protokollierung des Datenaustauschs

Auskunftsrecht

- Recht der betroffenen Personen

- Reproduzierbarkeit der Verfahren

Was ist der Oberbegriff "Schutzziele"

Der Oberbegriff "Schutzziele" bezieht sich auf die verschiedenen Ziele und Aspekte, die im Bereich der Informationssicherheit und des Datenschutzes verfolgt werden, um **Daten, Systeme und Informationen vor verschiedenen Bedrohungen zu schützen.** Diese **Schutzziele dienen als Leitlinien für Sicherheitsmaßnahmen und -richtlinien, um die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Systemen sicherzustellen**.

1. Vertraulichkeit

Unter Vertraulichkeit versteht man, dass **Daten nur von den Personen eingesehen oder offengelegt werden dürfen, die dazu auch berechtigt sind.** Will man Daten vertraulich behandeln, muss klar festgelegt werden, wer in welcher Art und Weise Zugriff auf diese Daten hat. Doch man muss noch einen weiteren Aspekt beachten, den viele gerne vergessen: Zur Vertraulichkeit von Daten gehört auch, dass diese bei der Übertragung nicht von unautorisierten Personen gelesen werden! Das heisst, es muss dafür gesorgt sein, dass die Daten bei einer Übertragung in geeigneter Weise verschlüsselt werden. Zu den verschiedenen Verschlüsselungsverfahren erfahren Sie hier mehr.

2. Integrität

Viele verwechseln Integrität mit Vertraulichkeit. Integrität bedeutet allerdings, **dass es nicht möglich sein darf, Daten unerkannt bzw. unbemerkt zu ändern.** Es geht hierbei also um das Erkennen von Datenänderungen, wohingegen bei Vertraulichkeit der Fokus auf der Berechtigung liegt. Oft wird mit Integrität (man spricht dann von starker Integrität) sogar gefordert, dass Daten überhaupt nicht unberechtigt verändert werden können. Da sich dies aber selten sinnvoll umsetzen lässt, empfehle ich die erste Definition. Nehmen wir einmal Forschungs- und Entwicklungsdaten. Wenn die Integrität solcher Daten zerstört ist, weil eine winzige Änderung unerkannt vorgenommen wurde, können Sie sämtlichen Daten nicht mehr trauen! Man muss niemandem erklären, dass dies eine Katastrophe wäre.

3. Verfügbarkeit

Die Verfügbarkeit eines Systems **beschreibt ganz einfach die Zeit, in der das System funktioniert.** Im Sinne der Schutzziele geht es hier selbstverständlich darum, die Verfügbarkeit möglichst hoch zu halten. Anders gesagt: Es gilt, das Risiko **Systemausfälle zu minimieren**!

Datenschutz	Datensicherheit
personenbezogene Daten	alle Daten
Schutz der informationellen Selbstbestimmung	Schutz vor Verlust, Zerstörung, etc.
gesetzliche Vorschriften	Technische Massnahmen / Lösungen selber finden

Vorteile (und Nachteile) eines Passwort-Manager

- Wird durch ein Master Passwort gesichert.
- Alle Passwörter sind an einer Stelle gesichert.
- Das Tool gibt Warnungen aus, wenn das Passwort zu schwach sein sollte und empfiehlt eines von sich aus.
- Kann auf mehreren Geräten genutzt werden, sowie auch Mobile (Apple, Android).

- (Bei Verlust vom Master Passwort hat man meist keine Möglichkeit mehr auf seine Datenbank zuzugreifen.)
- (Bei einem Hack auf die Datenbank werden dem Hacker alle Passwörter präsentiert.)

Die zwei Arten von Cookies

Ein Internet-Cookie ist eine kleine Textdatei, die von einer Website auf dem Computer eines Benutzers gespeichert wird, wenn er die Website besucht. Diese Datei enthält oft Informationen über die Interaktion des Benutzers mit der Website und dient verschiedenen Zwecken, darunter

- Sitzungsverwaltung: Cookies werden häufig verwendet, um Informationen über eine Benutzersitzung auf einer Website zu speichern. Dies ermöglicht es der Website, den Benutzer während seines Besuchs zu identifizieren und sicherzustellen, dass er angemeldet bleibt, während er die verschiedenen Seiten der Website durchsucht.
- Benutzerpräferenzen: Websites können Cookies verwenden, um Informationen über die Präferenzen eines Benutzers zu speichern, z. B. die Spracheinstellungen oder die gewünschte Anzeigeoption.
- Verfolgung von Aktivitäten: Einige Cookies werden verwendet, um das Verhalten der Benutzer auf einer Website zu verfolgen. Dies kann dazu beitragen, Benutzerprofile zu erstellen und personalisierte Inhalte oder Werbung bereitzustellen.
- Warenkorb und E-Commerce: Auf E-Commerce-Websites werden Cookies oft verwendet, um den Inhalt des Warenkorbs eines Benutzers zu speichern, damit er Produkte hinzufügen oder entfernen kann, während er auf der Website einkauft.
- Analyse und Tracking: Website-Betreiber verwenden Cookies auch, um Informationen über die Leistung ihrer Website zu sammeln, z. B. wie viele Besucher die Website hat und wie sie mit ihr interagieren. Dies hilft bei der Verbesserung der Website und der Benutzererfahrung.

Es ist wichtig zu beachten, dass es verschiedene Arten von Cookies gibt, darunter Sitzungscookies (die nach dem Schließen des Browsers gelöscht werden) und persistente Cookies (die auf dem Computer des Benutzers gespeichert bleiben, bis sie ablaufen oder gelöscht werden). Außerdem gibt es Datenschutzbedenken in Bezug auf Cookies, da sie dazu verwendet werden können, das Online-Verhalten von Benutzern zu verfolgen. Aus diesem Grund haben viele Länder und Regionen Datenschutzgesetze und -vorschriften erlassen, die die Verwendung von Cookies regeln.
Weitere Arten von Cookies. **Essenzielle bzw. notwendige Cookies:** Erforderlich für die Kernfunktionen einer Website, z.B. Benutzerauthentifizierung. **Funktionale Cookies:** Unterstützen zusätzliche Funktionen der Website, z.B. Spracheinstellungen oder Warenkorbinhalt. **Leistung- oder Performance Cookies:** Erfassen Daten zur Website-Nutzung, um die Leistung und Benutzererfahrung zu verbessern. **Tracking- und Werbe-Cookies:** Verfolgen das Online-Verhalten von Benutzern für personalisierte Werbung und Empfehlungen; umstritten in Bezug auf Datenschutz. **Erstanbieter-Cookies:** Cookies von der besuchten Website, speichern Website-spezifische Informationen wie Anmeldeinformationen. **Drittanbieter-Cookies:** Cookies von Drittanbietern, oft für Werbung und Tracking über verschiedene Websites hinweg. **Sicherheits-Cookies:** Erhöhen die Sicherheit von Websites, indem sie schädliche Aktivitäten erkennen oder Benutzer authentifizieren.

Was sind AGB, was ist ihr Inhalt, zähle vier Punkte auf...

Beim Verfassen der AGB sollten **alle Schritte des Verkaufsprozesses bedacht werden**. Hier einige Punkte, die es zu berücksichtigen gilt:

- **Gewährleistung**: Garantiebestimmungen, für die bei der Transaktion verkauften Waren oder Dienstleistungen.
- **Datenschutz**: Verwendung der gesammelten Daten, Verschlüsselungstechnik usw.
- **Bestellungen**: Rechnungs- und Zahlungsbedingungen, Mehrwertsteuer usw.
- **Lieferung**: Versandgebiete, Lieferfristen usw.
- **Haftung**: Beispielsweise im Falle einer Beschädigung der Ware während des Versands.
- **Retouren**: Umtausch- und Rücknahmeregelungen.
- **Anwendbares Recht und Gerichtsstand**: Im Streitfall zuständiges Gericht und anwendbares Recht (Verweis auf schweizerisches Recht).

Wie heisst der Service von Google der dir eine Page findet und was macht der SEO (Search-Engine-Optimization)

Der Service von Google, der dazu dient, eine bestimmte Seite (URL) im Internet zu finden, ist die Suchmaschine von Google selbst. Es gibt verschiedene Suchdienste von Google, darunter die bekannteste und am häufigsten verwendete ist die Google-Suche, die es Nutzern ermöglicht, Informationen im Internet zu finden, indem sie Schlüsselwörter eingeben, und somit richtige Domain findet zu der Seite die man vorhin gesucht hat.

SEO (Search Engine Optimization) bezieht sich auf die Praxis, die Qualität und Quantität des Traffics auf eine Website über organische Suchergebnisse, wie sie von Suchmaschinen wie Google, Bing, Yahoo, usw., angezeigt werden, zu verbessern. SEO beinhaltet verschiedene Techniken und Optimierungen, um die Sichtbarkeit einer Website in den Suchergebnissen zu erhöhen.

Das Hauptziel von SEO ist es, die Rankings einer Website in den Suchergebnissen zu verbessern, um mehr organischen Traffic anzuziehen und letztendlich die Sichtbarkeit und den Erfolg der Website im Internet zu steigern.

Datenschutzerklärung

Eine Datenschutzerklärung muss Antwort auf folgende Fragen geben können:

- Welche personenbezogenen Daten werden erhoben?
- Was passiert mit den erhobenen Daten?
- Warum werden überhaupt Daten erhoben?
- Werden die erhobenen Daten an Dritte weitergegeben?
- Findet ein grenzüberschreitender Datenverkehr statt?
- Welche Massnahmen werden zur Gewährleistung der Sicherheit der Daten ergriffen?

Impressum

- Name des Unternehmens oder der Organisation
- Vorname und Name der verantwortlichen Person
- Vollständige Postadresse; Postfach alleine reicht nicht
- E-Mail-Adresse

Empfehlenswert sind diese ergänzenden Angaben

- Rechtsform der Unternehmung
- Telefon- und Faxnummer
- ...

Zähle je zwei Vor- und Nachteile eines CMS-Systems (Webseite erstellen (WordPress, Jimdo))

Ein Content-Management-System (kurz CMS) ist eine Software, die zur Erstellung und Verwaltung von Inhalten – in Text-, Bild-, Video- oder sonstiger Form – verwendet wird. CMS werden vor allem zum Betreiben von Websites, aber auch für „Offline-Plattformen" (in Intranetzwerken) eingesetzt. Weit verbreitet sind vor allem Open-Source-Systeme, die sowohl professionelle als auch private Anwender nutzen. Insbesondere bei inhaltsreichen Web-Auftritten wie Onlineshops oder Medienportalen bietet sich eine Umsetzung mithilfe fein abgestimmter CMS an.

Vorteile:

1. **Benutzerfreundlichkeit:**
   - CMS-Systeme sind in der Regel benutzerfreundlich und erfordern keine tiefgreifenden technischen Kenntnisse. Inhalte können leicht erstellt, bearbeitet und verwaltet werden.
2. **Schnelle Inhaltsaktualisierung:**
   - Inhalte können schnell aktualisiert werden, was eine effiziente Pflege der Website ermöglicht, ohne auf Entwickler angewiesen zu sein.
3. **Vorlagen und Designs:**
   - Viele CMS bieten eine Vielzahl von Vorlagen und Designs, um das Erscheinungsbild der Website anzupassen, ohne von Grund auf neu zu beginnen.

Nachteile:

1. **Eingeschränkte Anpassungsmöglichkeiten:**
   - Oft sind CMS-Systeme in Bezug auf maßgeschneiderte Anpassungen und spezielle Funktionalitäten weniger flexibel.
2. **Sicherheitsrisiken:**
   - Da CMS weit verbreitet sind, können Sicherheitslücken und Schwachstellen in Plugins oder der Hauptplattform zu Sicherheitsrisiken führen, wenn sie nicht regelmäßig aktualisiert werden.
3. **Kosten und Lizenzierung:**
   - Einige fortschrittlichere CMS-Systeme können Lizenzgebühren erfordern, und die Implementierung und Anpassung können zusätzliche Kosten verursachen.

Wenn man das ISO-Zertifikat erhalten will, muss überprüft werden, ob die Prozesse eingehalten werden. Dazu gehört es auch die Daten zu klassifiziere. Klassifiziere nun die Daten (wie z.B. beim Überprüfungsprozess)

Die ISO/ IEC 27002 legt Richtlinien und allgemeine Grundsätze für die Einführung, Umsetzung, Aufrechterhaltung und Verbesserung des Informationssicherheits-Managements innerhalb einer Organisation fest.

Personenbezogene Daten können in verschiedene Kategorien unterteilt werden, abhängig von den Merkmalen und der Art der Daten. Bei der Analyse und Klassifizierung von personenbezogenen Daten sollten Datenschutzprinzipien und rechtliche Anforderungen berücksichtigt werden. Hier sind einige häufige Kategorien personenbezogener Daten:

- ❖ Identifikationsdaten
  - Vorname und Nachname
  - Geburtsdatum
  - Geschlecht
  - Sozialversicherungsnummer
  - Passnummer
  - Nationalität
- ❖ Kontaktinformationen
  - Adresse (privat, geschäftlich)
  - Telefonnummer (mobil, fest)
  - E-Mail-Adresse
  - Finanzdaten
  - Bankkontodaten
  - Kreditkarteninformationen
  - Finanztransaktionen
- ❖ Gesundheitsdaten
  - Medizinische Diagnosen
  - Krankengeschichte
  - Verschriebene Medikamente
- ❖ Biometrische Daten
  - Fingerabdrücke
  - Gesichts- oder Iriserkennung
  - DNA-Proben
- ❖ Nutzungsdaten
  - IP-Adressen
  - Geräteinformationen
  - Browserverlauf
  - Logins und Aktivitäten im Spiel
- ❖ Bild- und Videodate
  - Fotos
  - Videos
  - Audioaufnahmen
- ❖ Demografische Daten
  - Wohnort
  - Bildungsstand
  - Beruf
- ❖ Soziale Daten
  - Soziale Netzwerkprofile
  - Freundschaftslisten
  - Kommentare und Beiträge
- ❖ Verhaltensdaten
  - Vorlieben
  - Interessen
  - Kaufverhalten

Es ist wichtig zu betonen, dass die Kategorien und die Sensitivität der Daten je nach Kontext variieren können. Bei der Verarbeitung personenbezogener Daten müssen Datenschutzgesetze und -bestimmungen eingehalten werden, um die Privatsphäre und die Rechte der betroffenen Personen zu schützen. Die Analyse und Klassifizierung dieser Daten ermöglichen eine angemessene Handhabung, Speicherung und Übertragung gemäß den Datenschutzvorschriften.

Was macht man gegen Hacker-Angriffe. Welche Möglichkeiten gibt es sich zu wehren (Anti-Virus, Back-Up, Firewall, Personalschulungen, Code of Contact…)

Um Daten effektiv zu schützen, ist es wichtig, Sicherheitsmaßnahmen wie Verschlüsselung, regelmäßige Datensicherungen, Firewalls, Antivirensoftware, Schulungen zur Sensibilisierung der Benutzer und Sicherheitsrichtlinien zu implementieren.

Sie sollten sich also einen Überblick über die im Unternehmen vorhandenen Systeme und damit auch Datenbestände verschaffen.

Anschliessend müssen Sie analysieren, welche Systeme und Datenbestände unbedingt notwendig sind, damit die Arbeitsabläufe im Unternehmen funktionieren können. Diese sollten Sie entsprechend gegen Ausfälle schützen!

Eine Art Risikoanalyse, in der man Ausfallwahrscheinlichkeit, Ausfallzeit und Schadenspotenzial auflistet, ist hierbei zu empfehlen.

Zudem sollte die Geschäftsleitung bzw. eine Fachabteilung festlegen, welche Ausfallzeiten jeweils tolerierbar sind. Diese können nämlich von Unternehmen zu Unternehmen variieren. Beispielsweise kann es durchaus sein, dass der Ausfall des Mailservers für einen Tag verkraftbar ist; in anderen Unternehmen ist das der Super-GAU.

Risikoanalyse Bsp.

Besitzer	Szenario	Beschreibung	Ursache	Schadensklasse	Eintrittswahrscheinlichkeit
IT	Stromausfall	Serverfarmen können nicht mehr betrieben werden. Dienste stehen nicht mehr zur Verfügung.	kein Redundanz	hoch	mittel

Kennt Möglichkeiten zur Verschlüsselung von Daten auf dem eigenen Rechner (z.B. Datenträgerverschlüsselung).

Vollständige Festplattenverschlüsselung (Full Disk Encryption - FDE): Mit FDE können Sie die gesamte Festplatte oder SSD Ihres Computers verschlüsseln. Dies bedeutet, dass alle Daten, die auf dem Datenträger gespeichert sind, verschlüsselt werden, sodass sie nur mit einem Passwort oder einer Schlüsseldatei entschlüsselt werden können. Betriebssysteme wie Windows bieten BitLocker, macOS bietet FileVault, und es gibt auch Open-Source-Tools wie VeraCrypt, die für diese Zwecke verwendet werden können.

Datei- oder Verzeichnisverschlüsselung: Sie können auch wählen, bestimmte Dateien oder Verzeichnisse auf Ihrem Computer zu verschlüsseln, anstatt die gesamte Festplatte zu verschlüsseln. Dies ist nützlich, wenn Sie nur bestimmte Dateien oder Ordner schützen möchten. Werkzeuge wie Veracrypt oder EncFS bieten die Möglichkeit, einzelne Dateien oder Ordner zu verschlüsseln.

Cloud-Speicherverschlüsselung: Wenn Sie Cloud-Speicher-Dienste wie Dropbox, Google Drive oder OneDrive verwenden, können Sie Verschlüsselungstools wie Boxcryptor oder Cryptomator verwenden, um Ihre in der Cloud gespeicherten Daten zu schützen. Diese Tools verschlüsseln Ihre Dateien, bevor sie in die Cloud hochgeladen werden.

E-Mail-Verschlüsselung: Für die Verschlüsselung von E-Mails können Sie Tools wie PGP (Pretty Good Privacy) oder S/MIME verwenden, um Ihre E-Mail-Kommunikation zu schützen.

Verschlüsselung von USB-Laufwerken und externen Festplatten: Wenn Sie Daten auf USB-Laufwerken oder externen Festplatten speichern, können Sie diese mit Verschlüsselungssoftware wie VeraCrypt oder BitLocker (unter Windows) schützen.

Verschlüsselung von Archiven: Wenn Sie Dateiarchive erstellen, können Sie Tools wie 7-Zip verwenden, um die Archive mit einem Passwort zu schützen und die Dateien darin zu verschlüsseln.

EduGame will ein physisches Rechenzentrum (eigener Server) mit synchronisierter Cloud, was gibt es da zu optimieren. Nenne drei Optimierungs-Ideen.

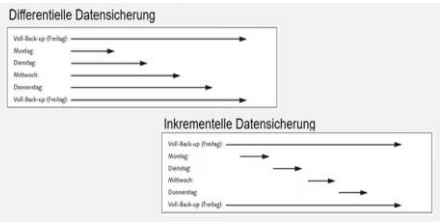
Dies Aufgabe ist im Prinzip die gleiche wie die Aufgabe 231-5A. Anhand dieser Aufgabe kann man verstehen, was in dieser Prüfungsfrage auch wirklich gefragt wird.

Aufgabe (231-5A)

- Welche Kriterien müssen bei der Wahl des Servers beachtet werden?
- Welchen Einfluss haben die Kriterien Redundanz, Backup und Archiv auf die Entscheidung?
- Welchen Einfluss hat die Wahl: Server im eigenen Rechenzentrum oder einen Server in der Cloud?
- Lassen sich die beiden Optionen miteinander kombinieren? Bitte begründen

Lösungsvorschlag

- Welche Kriterien müssen bei der Wahl des Servers beachtet werden?
  - Leistungsanforderungen
    - Der Server muss den erwarteten steigenden Besucherzahlen standhalten. Hierbei sind Aspekte wie Prozessorleistung, Arbeitsspeicher und Speicherkapazität zu berücksichtigen.
  - Redundanz
    - z.B. RAID1 für System, RAID5 für Daten
    - 2 Netzteile (1xUSV, 1xStadtnetz)
    - 2 CPU
    - Cluster
  - Backup (vollständig, inkrementell und differentielle)
    - Regelmäßige Backups sind notwendig, um Datenverluste zu vermeiden. Es ist wichtig zu prüfen, wie gut der Server für diese Prozesse ausgelegt ist.
    - Systemsicherung und -wiederherstellung
    - Datensicherung und -wiederherstellung
  - Performance
    - WAN-Anbindung
    - HDD, SSD
  - Skalierbarkeit
    - Die Fähigkeit, die Serverressourcen je na Bedarf zu erweitern, um den Anforderur des wachsenden Traffics gerecht zu wer
  - Sicherheit
    - Dies umfasst den Schutz vor Cyberangrif Datensicherheit sowie die Implementier von Verschlüsselungsprotokollen.



Optimierungsidee	Beschreibung
Betriebssystem und Software aktualisieren	Halten Sie Ihr Betriebssystem und Ihre Software auf dem neusten Stand, um sicher zu bleiben und die Leistung zu steigern
Sicherheitsmassnahmen ergreifen	Schützen Sie Ihren Server mit Firewalls und Intrusion Detection, um unerwünschte Zugriffe zu verhindern.
Load Balancing	Verteilen Sie den Datenverkehr gleichmässig auf verschiedene Server, um Überlastung zu vermeiden
Ressourcenüberwachung	Nutzen Sie Tools, um die Serverleistung im Auge zu behalten und Engpässe frühzeitig zu erkennen.
Cache verwenden	Speichern Sie oft angeforderte Daten zwischen, um die Antwortzeiten zu beschleunigen
Content Delivery Network (CDN)	Nutzen Sie CDNs, um Ihre Website schneller zu machen, indem Sie Inhalte auf Servern weltweit verteilen.
Datenbankoptimierung	Verbessern Sie Datenbankabfragen und Strukturen, um schnellere Antworten und Skalierbarkeit zu erzielen.
Virtualisierung	Nutzen Sie Virtualisierung, um Serverressourcen effizienter zu nutzen und flexibler zu sein.
Serverkonsolidierung	Reduzieren Sie die Serveranzahl, um Ressourcen zu optimieren und Kosten zu senken.
Lasttests	Testen Sie die Serverleistung unter Spitzenlast, um Engpässe frühzeitig zu identifizieren
Datensicherung und Wiederherstellung	Sichern Sie Ihre Daten, um Datenverlust zu verhindern, und stellen Sie sie im Notfall wieder her.
Energieeffizienz	Senken Sie den Energieverbrauch, indem Sie die Hardware optimieren und energieeffiziente Einstellungen nutzen.
Skalierbarkeit planen	Planen Sie für zukünftiges Wachstum mit redundanter Hardware und skalierbaren Lösungen.

- Welchen Einfluss haben die Kriterien Redundanz, Backup und Archiv auf die Entscheidung?
  - Redundanz
    - Die Website steht auch beim Ausfall eine Komponente weiterhin zur Verfügung, minimiert Ausfallzeiten.
  - Backup
    - System oder Daten bei einem Ausfall/Verlust wiederherstellen.
  - Archiv
    - Daten, wie z.B. Besucherzahlen, werden über 10 oder mehrere Jahre archiviert.
    - Können nicht mehr geändert werden.
- Welchen Einfluss hat die Wahl ob Server im eigenen RZ oder ein Server in der Cloud?

Die Wahl zwischen einem Server im eigenen Rechenzentrum oder in der Cloud hat verschiedene Auswirkungen:

Server im eigenen Rechenzentrum:

1. Kontrolle: Das Unternehmen behält die volle Kontrolle über die Infrastruktur.
2. Investitionen in Hardware und Wartung: Erfordert Investitionen in Hardware und Wartungskosten.
3. Skalierbarkeit: Die Skalierbarkeit kann begrenzt sein.

Server in der Cloud:

1. Skalierbarkeit: Bietet in der Regel eine bessere Skalierbarkeit je nach Bedarf.
2. Kosteneffizienz: Oft keine Vorabinvestitionen in Hardware, nutzungsabhängige Kosten.
3. Abhängigkeit vom Cloud-Anbieter: Es besteht eine gewisse Abhängigkeit vom Anbieter.

- Lassen sich die beiden Optionen miteinander kombinieren? Bitte begründe.
  - Die beiden Optionen (OnPremis oder Cloud) lassen sich miteinander kombinieren (Hybridansatz)
  - Kritische Systeme oder Daten werden im eigenen Rechenzentrum betrieben, während nicht-kritische Systeme oder solche, die eine höhere Skalierbarkeit erfordern, in der Cloud laufen.
  - Dies ermöglicht Flexibilität, Skalierbarkeit und die gleichzeitige Sicherheit kritischer Daten.

Um die beiden Optionen zu kombinieren, könnten Datenbanken und kritische Infrastruktur lokal im eigenen Rechenzentrum betrieben werden, während nicht-kritische Dienste wie das Tool zur Analyse der Besucherzahlen in der Cloud gehostet werden können.

Datenkategorie	Zu löschende Daten	Aufzubewahrende Daten	Nicht zu löschende Daten
Kontoinformationen	Benutzername, E-Mail-Adresse, Passwort, Profilbilder	Transaktionshistorie	Transaktionsdaten für Abrechnungszwecke
Personenbezogene Informationen	Vorname und Nachname, Geburtsdatum, Adresse, Telefonnummer, soziale Sicherheitsnummer	Kontaktinformationen für rechtliche Zwecke	Kontaktinformationen zur Erfüllung rechtlicher Anforderungen
Nutzerinhalte	Beiträge, Kommentare, Veröffentlichungen auf der Plattform	Supportverlauf	Aufzeichnung von Kundensupport-Anfragen
Kontakte und Verbindungen	Liste der Kontakte, Verbindungen zu anderen Nutzern	Backup-Daten	Backup-Daten zu den Verhinderungen von Datenverlust
Nutzungsdaten	Aktivitätsprotokolle, Transaktionshistorie, Suchverlauf	Aufbewahrungspflichten	Daten zur Einhaltung gesetzlicher Aufbewahrungspflichten
Kontoeinstellungen und Präferenzen	Benutzerpräferenzen, Benachrichtigungseinstellungen	Analytische Daten	Daten für analytische Zwecke in anonymisierter Form
Zahlungsinformationen	Kreditkartendaten, Zahlungsinformationen	Vertragsdaten	Verträge und Vereinbarungen zur rechtlichen Aufbewahrung
Cookies und Tracking-Daten	Cookies und Tracking-Informationen auf dem Gerät	Rechtliche Anforderungen	Informationen für rechtliche Anforderungen
Kommunikationsverläufe	Nachrichten, Chat mit anderen Nutzern		
Analyse- und Profiling-Daten	Daten für Analysezwecke, Nutzerprofile		
Einstellungen für Drittanbieter-Integrationen	Daten aus Drittanbieter-Integrationen		