Lernziele LB Modul 231

Inhalt

Prüfungsfragen

Insgesamt wird es 10 Fragen an der Prüfung geben. Eigentlich gibt es drei verschiedene LB's daher weiss man nicht ganz genau welche Fragen überhaupt und in welcher Reihenfolgen vorkommen.

Sonst auch wurden die Prüfungsfragen von Marc selber noch einmal auf Teams geschrieben worden

Beschreibe die drei A's (Authentifizierung – Authentisierung – Autorisierung) (3 Punkte)

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.[1]

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.

Zähle je zwei Vor- und Nachteile eines CMS-Systems (Webseite erstellen (WordPress, Jimdo)) (4 Punkte)

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.[2]

Vor- und Nachteile von CMS-Systemen:

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.
4. **Erweiterbarkeit durch Plugins:**
    - Durch die Verwendung von Plugins können zusätzliche Funktionen und Features leicht hinzugefügt werden, z. B. SEO-Tools, Sicherheitserweiterungen oder E-Commerce-Integrationen.
5. **Mehrbenutzerunterstützung:**
    - CMS ermöglichen oft mehreren Benutzern, gleichzeitig an der Website zu arbeiten, wobei verschiedene Zugriffsrechte vergeben werden können.
6. **SEO-Freundlichkeit:**

[1] (OneNote Modul 231, kein Datum)(231-2A Evaluation)
[2] (OneNote Modul 231, kein Datum)(231-3B Aufgabe 05.01)

- Viele CMS bieten Funktionen, die die Optimierung für Suchmaschinen vereinfachen, wie z.B. die Möglichkeit, Meta-Beschreibungen, Titel-Tags und URLs anzupassen.

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. **Performance-Einbußen:**
    - Einige CMS können bei umfangreichen und komplexen Websites oder bei übermäßiger Verwendung von Plugins an Leistung verlieren.
4. **Abhängigkeit von Updates:**
    - Regelmäßige Updates der Plattform und der Plugins sind erforderlich, um Sicherheit und Funktionalität aufrechtzuerhalten, was Zeit und Ressourcen erfordert.
5. **Kosten und Lizenzierung:**
    - Einige fortschrittlichere CMS-Systeme können Lizenzgebühren erfordern, und die Implementierung und Anpassung können zusätzliche Kosten verursachen.
6. **Lernkurve für Komplexität:**
    - Für komplexe Anpassungen oder spezielle Anforderungen kann die Einarbeitung in die Funktionsweise des CMS und die Umsetzung technischer Lösungen Zeit und Fachwissen erfordern.

Die Wahl eines CMS hängt von den spezifischen Anforderungen, dem Umfang der Website, dem Budget und den Fähigkeiten des Personals ab. Es ist wichtig, die Vor- und Nachteile abzuwägen, um die beste Lösung für die jeweiligen Bedürfnisse zu finden.[3]

Löschpflichtige und aufzubewahrende Daten, welche Daten sind es nach Datenschutzgesetz (4 Punkte)

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.

[3] (ChatGPT, kein Datum)

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). Für Beschäftigungsverhältnisse von praktischer Relevanz sind hierbei die Aufbewahrungs- und Dokumentationspflichten nach den Vorschriften des deutschen Arbeits-, Handels-, Sozialversicherungs- und Steuerrechts. Daneben kann gemäss Art. 17 Abs. 3e auch ein eigenes, berechtigtes Interesse (sog. Beweissicherungsinteresse) des Verantwortlichen an einer längeren Aufbewahrung bestehen (z.B. bei potenziellen Rechtsstreitigkeiten).

Grundsätzlich gilt hierbei: Spezialgesetzliche Aufbewahrungsfristen gehen stets den datenschutzrechtlichen Löschpflichten vor. Dementsprechend dürfen personenbezogene Daten nicht gelöscht werden, sofern derartige Aufbewahrungsfristen bestehen.[4]

Datenkategorie	Zu löschende Daten
1. Kontoinformationen	Benutzername, E-Mail-Adresse, Passwort, Profilbilder
2. Personenbezogene Informationen	Vorname und Nachname, Geburtsdatum, Adresse, Telefonnummer, soziale Sicherheitsnummer
3. Nutzerinhalte	Beiträge, Kommentare, Veröffentlichungen auf der Plattform
4. Kontakte und Verbindungen	Liste der Kontakte, Verbindungen zu anderen Nutzern
5. Nutzungsdaten	Aktivitätsprotokolle, Transaktionshistorie, Suchverlauf
6. Kontoeinstellungen und Präferenzen	Benutzerpräferenzen, Benachrichtigungseinstellungen
7. Zahlungsinformationen	Kreditkartendaten, Zahlungsinformationen
8. Cookies und Tracking-Daten	Cookies und Tracking-Informationen auf dem Gerät
9. Kommunikationsverläufe	Nachrichten, Chat mit anderen Nutzern
10. Analyse- und Profiling-Daten	Daten für Analysezwecke, Nutzerprofile
11. Einstellungen für Drittanbieter-Integrationen	Daten aus Drittanbieter-Integrationen

Aufzubewahrende Daten	Nicht zu löschende Daten
Transaktionshistorie	Transaktionsdaten für Abrechnungszwecke
Kontaktinformationen für rechtliche Zwecke	Kontaktinformationen zur Erfüllung rechtlicher Anforderungen
Supportverlauf	Aufzeichnung von Kundensupport-Anfragen
Backup-Daten	Backup-Daten zu den Verhinderungen von Datenverlust
Aufbewahrungspflichten	Daten zur Einhaltung gesetzlicher Aufbewahrungspflichten
Analytische Daten	Daten für analytische Zwecke in anonymisierter Form
Vertragsdaten	Verträge und Vereinbarungen zur rechtlichen Aufbewahrung
Rechtliche Anforderungen	Informationen für rechtliche Anforderungen

[4] (OneNote Modul 231, kein Datum)(231-4A)

EduGame will ein physisches Rechenzentrum (eigener Server) mit synchronisierter Cloud, was gibt es da zu optimieren. Nenne drei Optimierungs-Ideen. (12 Punkte)

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.

Ausgangslage

Die Geschäftsleitung der EduGame AG hat entschieden, den eigenen Webauftritt zu überarbeiten. Auf der neuen Website können sich sowohl Partner wie auch Kunden registrieren, Produkte kaufen und verkaufen. Der neue Webauftritt geht somit weit über eine klassische Website hinaus, wo einfach nur das Unternehmen präsentiert wird. Aufgrund der neuen Funktionalitäten wird mit stark steigenden Besucherzahlen auf der neuen Website gerechnet.

Aus diesem Entscheid resultieren zwei Aufträge. Ein Auftrag zur Erarbeitung der Designvorschläge geht an die Marketingabteilung und ein weiterer Auftrag zur Evaluation der Infrastruktur geht an die IT-Abteilung. Letzteren Auftrag übernimmst du.

Bisher werden die IT-Systeme in den eigenen (eingemieteten) Rechenzentren betrieben. Eine Option wäre somit, den Webserver ebenfalls in diesen Rechenzentren zu betreiben. Hier gilt es zu prüfen, ob der neue Webserver auf der bestehenden Infrastruktur betrieben werden kann oder ob ein neuer Server angeschafft werden muss. Aufgrund der Tatsache, dass die Geschäftsleitung offen ist, Dienste neu auch aus der Cloud zu beziehen, ist dies eine weitere Option. Ein Mischbetrieb (OnPrem und Cloud) wäre ebenfalls denkbar.

Daten, welche von den Kunden oder Partnern eingegeben werden, werden in der bestehenden Datenbank gespeichert. Die Datenbank wird auf einem Server in den eigenen Rechenzentren betrieben. Die Datenbank soll nicht erneuert werden.

Zur Analyse der Besucherzahlen und des Surfverhaltens wird ein Tool inkl. Datenbank auf dem Webserver installiert. Die Daten sollen mindestens 20 Jahre verfügbar sein.

Aufgabe

- 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[5]

Lösungsvorschlag

Der Lösungsvorschlag dient als Ideenpool und ist nicht abschliessend.

- Welche Kriterien müssen bei der Wahl des Servers beachtet werden?
  - Redundanz
    - z.B. RAID1 für System, RAID5 für Daten
    - 2 Netzteile (1xUSV, 1xStadtnetz)
    - 2 CPU
    - Cluster
  - Backup
    - Systemsicherung und -wiederherstellung
    - Datensicherung und -wiederherstellung

[5] (OneNote Modul 231, kein Datum)(231-5A Aufgabe)

    - Performance
        - WAN-Anbindung
        - HDD, SSD
- Welchen Einfluss haben die Kriterien Redundanz, Backup und Archiv auf die Entscheidung?
    - Redundanz
        - Die Website steht auch beim Ausfall einer Komponente weiterhin zur Verfügung.
    - 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?
    - Reicht die zur Verfügung stehende Bandbreite?
    - Wird der Webserver in den eigenen RZs betrieben?

- Lassen sich die beiden Optionen miteinander kombinieren? Bitte begründe.
    - Die beiden Optionen (OnPremis oder Cloud) lassen sich miteinander kombinieren.
    - Für eine bessere Ausfallssicherheit.[6]

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

[6] (OneNote Modul 231, kein Datum)(231-5A Evaluation)

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.

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)

Daten müssen klassifiziert werden wie bei den Lösungen von Aufgabe 231-6A –(Identifikationsdaten, Kontaktdaten…) (Fallbeispiel Steam) (OneNote).

Die ISO/ IEC 27002 legt Richtlinien und allgemeine Grundsätze für die Einführung, Umsetzung, Aufrechterhaltung und Verbesserung des Informationssicherheits-Managements innerhalb einer Organisation fest.[7]

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:

1. Identifikationsdaten
   - Vorname und Nachname
   - Geburtsdatum
   - Geschlecht
   - Sozialversicherungsnummer
   - Passnummer
   - Nationalität
2. Kontaktinformationen
   - Adresse (privat, geschäftlich)
   - Telefonnummer (mobil, fest)
   - E-Mail-Adresse
3. Finanzdaten
   - Bankkontodaten
   - Kreditkarteninformationen
   - Finanztransaktionen
4. Gesundheitsdaten
   - Medizinische Diagnosen
   - Krankengeschichte
   - Verschriebene Medikamente
5. Biometrische Daten
   - Fingerabdrücke
   - Gesichts- oder Iriserkennung
   - DNA-Proben

[7] (OneNote Modul 231, kein Datum)(231-1A Aufgabe 02.03)

6. Nutzungsdaten
   - IP-Adressen
   - Geräteinformationen
   - Browserverlauf
   - Logins und Aktivitäten im Spiel
7. Bild- und Videodate
   - Fotos
   - Videos
   - Audioaufnahmen
8. Demografische Daten
   - Wohnort
   - Bildungsstand
   - Beruf
9. Soziale Daten
   - Soziale Netzwerkprofile
   - Freundschaftslisten
   - Kommentare und Beiträge
10. 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.[8]

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

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.

[8] (OneNote Modul 231, kein Datum)(231-6A Evaluation)

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

[9]

Des Weiteren sollten folgende Punkte beachtet werden:

- Firewall
- Antiviren Software
- Verschlüsselung
- VPN
- Sichere Benutzerkonten (Passwortkomplexität)
- BACKUP in die Cloud

Es gibt Dienstleister, die die IT unter die Lupe nehmen und einen Hackangriff durchführen. Solche Hacker sind White-Hat-Hacker und geben eine saubere Übersicht, wie sicher ein Unternehmen ist. [10]

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).[11]

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

1. Sitzungsverwaltung: Cookies werden häufig verwendet, um Informationen über eine Benutzersitzung auf einer Website zu speichern. Dies ermöglicht es der Website, den Benutzer

[9] (OneNote Modul 231, kein Datum)(231-4B Evaluation)
[10] (OneNote Modul 231, kein Datum)(231-1A Evaluation)
[11] (OneNote Modul 231, kein Datum)(231-3A Evaluation)

während seines Besuchs zu identifizieren und sicherzustellen, dass er angemeldet bleibt, während er die verschiedenen Seiten der Website durchsucht.

2. Benutzerpräferenzen: Websites können Cookies verwenden, um Informationen über die Präferenzen eines Benutzers zu speichern, z. B. die Spracheinstellungen oder die gewünschte Anzeigeoption.

3. 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.

4. 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.

5. 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.[12]

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 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**.[13]

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

[12] (OneNote Modul 231, kein Datum)(231-3C Evaluation)
[13] (ChatGPT, kein Datum)

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**![14]

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

[14] (OneNote Modul 231, kein Datum)(231-4B Evaluation)

Auskunftsrecht

- Recht der betroffenen Personen
- Reproduzierbarkeit der Verfahren[15]

Vorteil eines Passwort-Manager

Vorteil:

- 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).

Nachteil:

- 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.[16]

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

Diese Prüfungsfrage ist an die Aufgabe 231-8A in OneNote angelehnt.

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.

Einige Schlüsselaspekte von SEO umfassen:

1. Keyword-Optimierung: Verwendung relevanter Schlüsselwörter, die von Benutzern in Suchmaschinen eingegeben werden.
2. On-Page-Optimierung: Verbesserung von Inhalten, Meta-Tags, Bilder und Struktur der Website, um Suchmaschinenfreundlichkeit zu erhöhen.
3. Off-Page-Optimierung: Erhöhung der Autorität einer Website durch den Aufbau von Backlinks und Erwähnungen von anderen vertrauenswürdigen Quellen im Internet.
4. Technische Optimierung: Gewährleistung einer reibungslosen Funktionsweise der Website, schnelle Ladezeiten und mobile Optimierung.

[15] (OneNote Modul 231, kein Datum)(231-6A Aufgabe 02.06)
[16] (OneNote Modul 231, kein Datum)(231-1B Evaluation)

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.[17]

Lernziele (nach HANOK)

Kennt verschiedene Kategorien der Schutzwürdigkeit von Daten und deren Kriterien.

1. Das Datenschutzrecht unterscheidet zwischen vielen verschiedenen Kategorien. Dazu gehören:

    - Allgemeine Personendaten
        - Kriterien: Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies kann Namen, Geburtsdaten, Sozialversicherungsnummern, Adressen, Telefonnummern und ähnliche Informationen umfassen.[18]
    - Kennnummern
    - Bankdaten
        - Kriterien: Daten, die finanzielle Informationen einer Person oder Organisation betreffen, einschließlich Bankkontoinformationen, Kreditkartennummern, Gehaltsdaten und Steuererklärungen.[19]
    - Patientendaten
        - Kriterien: Daten, die Informationen über die physische oder geistige Gesundheit einer Person enthalten. Dies kann medizinische Aufzeichnungen, Diagnosen, Behandlungen und genetische Informationen einschließen.[20]
    - physische Merkmale
    - oder Besitzmerkmale[21]

Kennt den Unterschied von Datenschutz und Datensicherheit

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

[22]

Kennt verschiedene Rechtsräume (Schweiz, EU)

Es gibt unterschiedliche Rechtsräume und rechtliche Rahmenbedingungen in verschiedenen Regionen und Ländern, darunter die Schweiz und die Europäische Union (EU).

Es ist wichtig zu beachten, dass sowohl die Schweiz als auch die EU strenge Datenschutzvorschriften haben, aber die spezifischen **Gesetze und Regelungen in jedem Rechtsraum variieren können.** Unternehmen und Organisationen, die in diesen Regionen tätig sind oder personenbezogene Daten

[17] (ChatGPT, kein Datum)
[18] (ChatGPT, kein Datum)
[19] (ChatGPT, kein Datum)
[20] (ChatGPT, kein Datum)
[21] (OneNote Modul 231, kein Datum)(231-1A Evaluation)
[22] (OneNote Modul 231, kein Datum)(231-1A Evaluation)

von Personen in diesen Regionen verarbeiten, müssen die jeweiligen Datenschutzbestimmungen und -anforderungen beachten.[23]

Kennt für den jeweiligen Rechtsraum die juristischen Werke (z. B. DSG, DSGVO).

Die Schweiz hat ein strenges Datenschutzregime, das hauptsächlich im Bundesgesetz über den **Datenschutz (DSG)** geregelt ist. Die **Datenschutzbehörde**, der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)**, überwacht und reguliert den Datenschutz in der Schweiz.

Obwohl die Schweiz nicht Mitglied der EU ist, hat sie die **DSGVO** in gewissem Maße übernommen. Dies erleichtert den grenzüberschreitenden Datentransfer zwischen der Schweiz und EU-Ländern.

Die EU hat die DSGVO eingeführt, um einheitliche Datenschutzregeln in allen EU-Mitgliedstaaten zu schaffen. Die DSGVO legt strenge Vorschriften für die Verarbeitung personenbezogener Daten fest und stärkt die Rechte der Einzelpersonen in Bezug auf ihre Daten.[24]0

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

es gibt verschiedene Möglichkeiten zur Verschlüsselung von Daten auf Ihrem eigenen Rechner, einschließlich der Verschlüsselung von Datenträgern. Hier sind einige gängige Methoden zur Datenverschlüsselung auf Ihrem Computer:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.

[23] (ChatGPT, kein Datum)
[24] (ChatGPT, kein Datum)

Es ist wichtig zu beachten, dass Sie Ihre Verschlüsselungspasswörter und Schlüssel sicher aufbewahren müssen, da Sie auf Ihre verschlüsselten Daten nicht zugreifen können, wenn Sie Ihre Zugangsdaten verlieren. Die Wahl des richtigen Verschlüsselungswerkzeugs hängt von Ihren speziellen Anforderungen und Ihrem Betriebssystem ab. Stellen Sie sicher, dass Sie die Anweisungen des jeweiligen Werkzeugs genau befolgen, um Ihre Daten effektiv zu schützen.[25]

Kennt Verfahren zur Erstellung und Wiederherstellung von Backups.

Klassifizierung der Daten

Überlegen Sie sich deswegen als erstes, auf welchen Geräten Sie überall persönliche Daten gespeichert haben und versuchen Sie diese zu klassifizieren. Auf Ihrem Computer gilt es, die wichtigen Dateien und Ordner zu identifizieren.

Die richtige Backup-Methode

Es gibt unterschiedliche Methoden, wie Sie Ihre Daten sichern können. Dabei gibt es einige Faktoren, welche die Auswahl der richtigen Methode beeinflussen, wie etwa die Größe der zu sichernden **Datenmenge**, **Kosten** für die Datenträger, Ihre **Anbindung ans Internet** oder die **Häufigkeit von Änderungen.**

Vollständiges Backup

Das vollständige Backup sichert, wie es der Name bereits verrät, Ihren kompletten Datenbestand beziehungsweise Ihre komplette Festplatte. Dies umfasst sowohl Ihre persönlichen Daten, als auch die Daten des Betriebssystems.

- Einfache Sicherung
- Keine Backup-Strategie notwendig
- Stetig steigender Platzbedarf
- Zeitlich hoher Sicherungsaufwand

Differentielles Backup

Bei der differentiellen Datensicherung wird am ersten Tag eine vollständige Datensicherung gemacht, an den darauffolgenden Tagen sichern Sie nur die veränderten Daten. Die Veränderungen werden immer in Bezug zur Vollsicherung gemacht. Damit wächst das differentielle Backup stetig an, bis Sie wieder eine vollständige Sicherung durchführen.

- Benötigt weniger Speicherplatz als Vollsicherung
- Schneller als Vollsicherung
- Geänderte Dateien werden bis zur nächsten Vollsicherung jedes Tag gesichert
- Wiederherstellung langsamer als Vollsicherung
- Zwei Daten zur Wiederherstellung notwendig
- Für die differentielle Sicherung ist ebenfalls ein Backup-Client notwendig.

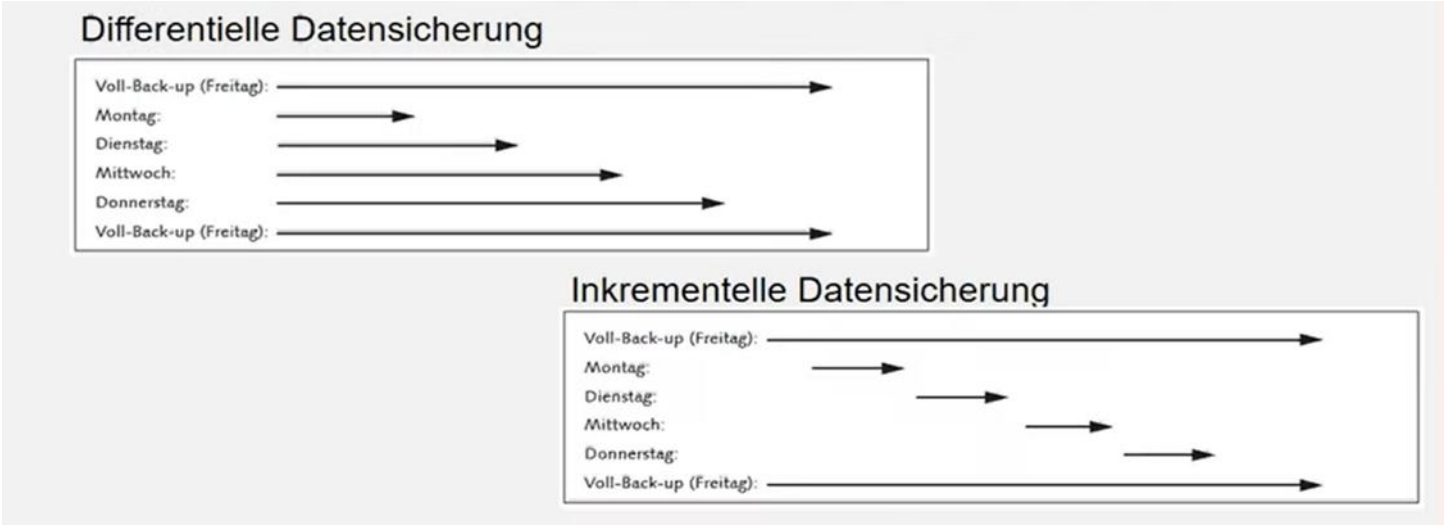
Inkrementelles Backup

Beim inkrementellen Backup starten Sie ebenfalls wie beim differentiellen Backup mit einer Vollsicherung Ihrer Daten. In den nächsten Sicherungen werden dann jeweils nur die Änderungen gesichert, die seit dem letzten Backup passiert sind. Dabei spielt es keine Rolle, ob dies die Vollsicherung oder eine inkrementelle Sicherung war.

- ist eines der inkrementellen Backups defekt, können alle weiteren Backups auch nicht mehr eingespielt werden.
- Geringer Speicherbedarf

[25] (ChatGPT, kein Datum)

- Schnelles Backup nach initialer Vollsicherung
- Wiederherstellung aufwändig und risikobehaftet



Mehrgenerationen-Prinzip

Beim diesem Vorgehen werden mehrere Sicherungen in unterschiedlichen Abstufungen – Großvater, Vater und Sohn – erzeugt. Ziel dabei ist es, verschiedene Versionsstände für die Wiederherstellung verfügbar zu haben.

Das Mehrgenerationen-Prinzip ist nicht an einen bestimmte Backup-Methode gebunden sondern zeigt eine Möglichkeit auf, wie Sie mit einer bestimmten Anzahl von Speichermedien eine optimale Rotation der Speichermedien erzielen.

Das Prinzip wird vor allem bei überschreibbaren Medien wie Bändern oder Sicherungskassetten angewandt.

3-2-1 Regel

Eine Regel, die Ihnen auch immer wieder begegnen wird, wenn Sie sich mit dem Thema Backup-Strategien beschäftigen, ist die 3-2-1 Regel. Was verbirgt sich dahinter?

- Die 3 steht für die dreifache Speicherung Ihrer Daten: einmal als Original im Live-System und ergänzend dazu auf zwei alternativen Speichermedien.
- Die 2 steht für die Datensicherung auf zwei unterschiedlichen Technologien. Die können beispielsweise eine externe USB-Festplatte, ein Netzwerk-Speicher (NAS – Network Attached Storage), eine Blu-Ray oder ein Cloudspeicher sein. Mehr zu den einzelnen Speichertypen, den Kosten sowie den Einsatzgebieten erfahren Sie in den folgenden Abschnitten.
- Die 1 steht für eine Datensicherung außer Haus. Dies kann beispielsweise die Cloud sein oder bei Ihnen in der Firma.

Wenn Sie diese Regel und die dazu passende Backup-Methode kombinieren, kann Ihren Daten nichts mehr passieren.[26]

Wiederherstellung von Backups

1. **Notfallwiederherstellung:** Bei einem Datenverlust oder einem Systemausfall können Sie ein vollständiges Backup verwenden, um Ihr System in seinem vorherigen Zustand wiederherzustellen.

[26] (OneNote Modul 231, kein Datum)(231-5A Aufgabe 02.01)

2. **Selektive Wiederherstellung:** In einigen Fällen müssen Sie möglicherweise nur bestimmte Dateien oder Verzeichnisse aus einem Backup wiederherstellen. Backup-Software ermöglicht normalerweise eine selektive Wiederherstellung.

3. **Prüfung und Validierung:** Nach der Wiederherstellung sollten Sie Ihre Daten auf Genauigkeit und Integrität prüfen, um sicherzustellen, dass die Wiederherstellung erfolgreich war.

4. **Notfallplan:** Es ist ratsam, einen Notfallwiederherstellungsplan zu erstellen, der beschreibt, wie im Falle eines Systemausfalls oder Datenverlusts vorgegangen wird. Dies kann die Wiederherstellung von Backups und die Schritte zur Minimierung von Ausfallzeiten umfassen.

5. **Testwiederherstellung:** Es ist wichtig, regelmäßig Testwiederherstellungen durchzuführen, um sicherzustellen, dass Ihre Backups ordnungsgemäß funktionieren. Dies ist besonders wichtig in geschäftlichen Umgebungen.

Die Erstellung und Wiederherstellung von Backups sind entscheidend, um Datenverlust und Betriebsausfälle zu verhindern. Es ist wichtig sicherzustellen, dass Backups regelmäßig durchgeführt werden, dass sie ordnungsgemäß verschlüsselt und geschützt sind und dass Sie wissen, wie Sie im Notfall auf sie zugreifen und sie wiederherstellen können.[27]

Kennt Techniken des Zugriffsschutzes, Passwortmanager und Prinzipien der Passwortverwaltung

Ja, es gibt verschiedene Techniken des Zugriffsschutzes, Passwortmanager und Prinzipien der Passwortverwaltung, die dazu dienen, den Zugriff auf digitale Konten und Informationen zu sichern. Hier sind einige grundlegende Konzepte und Techniken:

Techniken des Zugriffsschutzes:

1. **Passwörter:** Passwörter sind die häufigste Methode zum Schutz von digitalen Konten. Sie bestehen aus einer Kombination aus Buchstaben, Zahlen und Sonderzeichen. Es ist wichtig, starke, einzigartige Passwörter zu verwenden und sie regelmäßig zu ändern.

2. **Zwei-Faktor-Authentifizierung (2FA):** 2FA fügt eine zusätzliche Sicherheitsebene hinzu, indem Benutzer neben ihrem Passwort einen zweiten Faktor, wie z. B. einen Einmalcode, ein Fingerabdruck oder ein Hardware-Token, verwenden müssen.

3. **Biometrische Authentifizierung:** Biometrische Merkmale wie Fingerabdrücke, Gesichtserkennung oder Iris-Scans können zur Identifizierung und Authentifizierung von Benutzern verwendet werden.

4. **Single Sign-On (SSO):** SSO ermöglicht es Benutzern, sich mit einem einzigen Satz von Anmeldedaten bei mehreren Diensten oder Anwendungen anzumelden, was die Verwaltung von Zugriffsdaten vereinfacht.

5. **Zugriffssteuerungslisten (ACLs):** ACLs legen fest, welche Benutzer oder Gruppen von Benutzern auf bestimmte Ressourcen zugreifen können. Sie sind häufig in Netzwerken und auf Servern zu finden.

Passwortmanager:

[27] (ChatGPT, kein Datum)

1. **Passwort-Manager-Software:** Passwortmanager sind spezielle Programme oder Anwendungen, die dazu dienen, Passwörter sicher zu speichern und zu verwalten. Sie können starke, zufällige Passwörter generieren und für verschiedene Konten speichern.
2. **Sichere Speicherung:** Passwortmanager speichern Ihre Passwörter verschlüsselt und schützen sie mit einem Hauptpasswort oder einer anderen Form der Authentifizierung.
3. **Automatisches Ausfüllen:** Passwortmanager können Anmeldeinformationen automatisch in Websites und Apps eintragen, was die Bequemlichkeit erhöht.

Prinzipien der Passwortverwaltung:

1. **Verwenden Sie starke, einzigartige Passwörter:** Vermeiden Sie einfache Passwörter und verwenden Sie verschiedene Passwörter für verschiedene Konten.
2. **Ändern Sie Passwörter regelmäßig:** Es ist ratsam, Passwörter von Zeit zu Zeit zu ändern, insbesondere für sensible Konten.
3. **2FA aktivieren:** Wenn möglich, aktivieren Sie die Zwei-Faktor-Authentifizierung, um die Sicherheit Ihrer Konten zu erhöhen.
4. **Verwenden Sie einen Passwortmanager:** Ein Passwortmanager erleichtert die Verwaltung von Passwörtern und ermöglicht die Verwendung von komplexen, zufälligen Passwörtern.
5. **Überprüfen Sie die Sicherheit Ihrer Passwörter:** Nutzen Sie Tools, um die Stärke Ihrer Passwörter zu überprüfen und potenzielle Schwachstellen zu identifizieren.
6. **Teilen Sie keine Passwörter:** Teilen Sie niemals Ihre Passwörter mit anderen Personen, es sei denn, es ist unbedingt erforderlich.
7. **Sicherung Ihrer Passwörter:** Stellen Sie sicher, dass Sie Ihre Passwörter sicher aufbewahren und bei Bedarf eine Sicherungskopie erstellen.

Durch die Anwendung dieser Prinzipien und Techniken können Sie dazu beitragen, die Sicherheit Ihrer digitalen Konten und Informationen zu gewährleisten.[28]

Kennt den Unterschied von Authentifizierung und Autorisierung

Da diese drei Begriffe eng miteinander zusammenhängen und häufig verwechselt werden, erklären wir sie in einem Eintrag. Authentisierung bezeichnet das Nachweisen einer Identität. Authentifizierung bezeichnet die Prüfung dieses Identitätsnachweises auf seine Authentizität. Autorisierung bezeichnet das Gewähren des Zugangs zu den Privilegien, welche der erfolgreich nachgewiesenen Identität zustehen.

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

[28] (ChatGPT, kein Datum)

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.[29]

Kennt Verfahren zur Speicherung von Daten und bewusst redundanter Datenhaltung (z. B. lokal, Server, Cloud)

Die Speicherung von Daten und bewusst redundante Datenhaltung sind wichtige Konzepte in der Datenverwaltung und Datensicherheit. Hier sind einige Verfahren zur Speicherung von Daten und zur Implementierung redundanter Datenhaltung in verschiedenen Umgebungen, einschließlich lokaler Speicherung, Servern und der Cloud:

Lokale Speicherung:

1. **Festplatten und SSDs:** Lokale Speichergeräte wie Festplatten und Solid-State-Laufwerke (SSDs) werden oft verwendet, um Daten auf einem einzelnen Computer oder Server zu speichern. Daten können auf diesen Geräten redundant gespeichert werden, indem sie in RAID-Arrays (Redundant Array of Independent Disks) organisiert werden, um Datenverlust bei Festplattenausfällen zu verhindern.
2. **Externe Festplatten und USB-Laufwerke:** Externe Festplatten und USB-Laufwerke dienen zur Sicherung und mobilen Datenübertragung. Daten können auf mehreren externen Laufwerken gespiegelt oder gesichert werden.
3. **Netzwerklaufwerke:** Netzwerklaufwerke, auch NAS (Network Attached Storage) genannt, ermöglichen den gemeinsamen Zugriff auf Daten in einem lokalen Netzwerk. Daten können auf NAS-Geräten redundant gespeichert werden.

Serverumgebungen:

1. **Datenbankreplikation:** In Serverumgebungen werden Datenbanken oft repliziert, um eine redundante Datenhaltung sicherzustellen. Dies ermöglicht die Skalierbarkeit und Verfügbarkeit von Daten.
2. **Load Balancer:** Load Balancer verteilen den Datenverkehr auf mehrere Server, um eine hohe Verfügbarkeit und Lastverteilung zu gewährleisten. Dies kann auch als eine Form der Datenredundanz angesehen werden.
3. **Backup-Server:** Backup-Server speichern Kopien von Daten in regelmäßigen Abständen, um Datenverlust bei Serverausfällen oder Datenkorruption zu verhindern.

Cloud-Umgebungen:

[29] (OneNote Modul 231, kein Datum)(231-2A Evaluation)

1. **Datenreplikation:** Cloud-Anbieter bieten oft automatische Datenreplikation über mehrere Rechenzentren hinweg, um die Verfügbarkeit und Sicherheit von Daten zu gewährleisten.
2. **Datenarchivierung:** Cloud-Dienste ermöglichen die Archivierung von Daten, um sicherzustellen, dass sie bei Verlust oder versehentlicher Löschung wiederhergestellt werden können.
3. **Redundante Regionen:** Einige Cloud-Anbieter bieten redundante Rechenzentrumsregionen an verschiedenen geografischen Standorten an, um eine zusätzliche Schicht der Datenredundanz und Geschäftskontinuität bereitzustellen.
4. **Hybrid Cloud:** Unternehmen können hybride Cloud-Umgebungen einrichten, bei denen Daten sowohl in der öffentlichen Cloud als auch in privaten Rechenzentren gespeichert werden, um die Vorteile beider Ansätze zu nutzen.

Redundante Datenhaltung ist ein wichtiger Bestandteil der Datensicherheit und Geschäftskontinuität. Sie stellt sicher, dass Daten auch dann verfügbar sind, wenn einzelne Komponenten ausfallen oder unzugänglich werden. Die Wahl der richtigen Speichermethode und Redundanzstrategie hängt von den spezifischen Anforderungen, dem Budget und den Risikotoleranzen ab.[30]

Kennt verschiedene Gefahren, denen Daten ausgesetzt sind (z.B. Diebstahl, Ransomware, Integritätsverletzung).

Daten sind in der heutigen digitalen Welt verschiedenen Gefahren ausgesetzt. Hier sind einige der häufigsten Gefahren, denen Daten ausgesetzt sein können:

1. **Diebstahl:** Daten können gestohlen werden, sei es physisch durch den Diebstahl von Geräten wie Laptops oder Servern oder digital durch unbefugten Zugriff auf Computersysteme oder Netzwerke.
2. **Ransomware:** Ransomware ist eine Art von Schadsoftware, die Daten verschlüsselt und Lösegeld von den Opfern verlangt, um die Daten wiederherzustellen. Wenn das Lösegeld nicht gezahlt wird, können die Daten verloren gehen.
3. **Malware:** Malware (schädliche Software) kann dazu verwendet werden, Daten zu stehlen, zu beschädigen oder zu manipulieren. Dies kann Spyware, Viren, Würmer und Trojaner umfassen.
4. **Phishing:** Bei Phishing-Angriffen werden gefälschte E-Mails oder Websites verwendet, um Benutzer zur Preisgabe sensibler Daten wie Benutzernamen und Passwörtern zu verleiten.
5. **Hacking und unbefugter Zugriff:** Angreifer können versuchen, sich unbefugten Zugriff auf Computersysteme, Netzwerke oder Online-Konten zu verschaffen, um Daten zu stehlen oder zu manipulieren.
6. **Social Engineering:** Bei dieser Methode manipulieren Angreifer Menschen, um vertrauliche Informationen preiszugeben. Dies kann durch Täuschung, Betrug oder Manipulation erfolgen.

[30] (ChatGPT, kein Datum)

7. **Datenlecks:** Datenlecks können durch menschliche Fehler oder Schwachstellen in Systemen verursacht werden. Infolge von Datenlecks werden vertrauliche Informationen versehentlich oder absichtlich veröffentlicht.
8. **Physische Schäden:** Daten können durch Naturkatastrophen wie Überschwemmungen, Brände oder Erdbeben gefährdet sein, wenn die physische Infrastruktur beschädigt wird.
9. **Integritätsverletzungen:** Eine Integritätsverletzung tritt auf, wenn Daten absichtlich oder unbeabsichtigt geändert werden, was zu Datenkorruption oder Manipulation führt.
10. **Datenverlust:** Daten können aufgrund von technischen Ausfällen, Hardwareproblemen oder versehentlicher Löschung verloren gehen.
11. **Datenspeicherprobleme:** Probleme mit Datenspeichergeräten, wie Festplatten oder SSDs, können zum Verlust oder zur Beschädigung von Daten führen.
12. **Wirtschaftsspionage:** In diesem Fall versuchen Angreifer, sensible Unternehmensdaten oder geistiges Eigentum zu stehlen, um Wettbewerbsvorteile zu erlangen.
13. **Rechtliche und Compliance-Risiken:** Unternehmen und Organisationen müssen Daten nach geltenden Gesetzen und Vorschriften schützen, da Verstöße zu rechtlichen Konsequenzen führen können.

Um Daten effektiv zu schützen, ist es wichtig, Sicherheitsmaßnahmen wie Verschlüsselung, regelmäßige Datensicherungen, Firewalls, Antivirensoftware, Schulungen zur Sensibilisierung der Benutzer und Sicherheitsrichtlinien zu implementieren. Datenschutz und Datensicherheit sind entscheidend, um Daten vor den oben genannten Gefahren zu schützen.[31]

Kennt wesentliche Unterschiede in den Datenschutzgesetzen der verschiedenen Rechtsräume.

Es gibt wesentliche Unterschiede in den Datenschutzgesetzen und -vorschriften in verschiedenen Rechtsräumen weltweit. Diese **Unterschiede können in den Definitionen, Anforderungen, Fristen und Sanktionen** im Bereich des Datenschutzes liegen.

Diese Unterschiede in den Datenschutzgesetzen und -vorschriften zwischen verschiedenen Rechtsräumen erfordern von Unternehmen und Organisationen, die international tätig sind oder personenbezogene Daten verarbeiten, die Einhaltung der spezifischen Anforderungen jedes Rechtsraums, um rechtliche und regulatorische Risiken zu minimieren. Folgende Datenschutzgesetze sind für uns am wichtigsten:

DSG (Datenschutzgesetz) in der Schweiz

Das Schweizer Datenschutzgesetz (DSG) regelt den Umgang mit personenbezogenen Daten in der Schweiz. Es definiert die Rechte und Pflichten von Organisationen im Umgang mit personenbezogenen Daten und schützt die Privatsphäre der Einzelpersonen. Das DSG ähnelt in einigen Aspekten der DSGVO (Europäische Datenschutz-Grundverordnung), weist jedoch auch spezifische Unterschiede auf, insbesondere in Bezug auf den Geltungsbereich und die Anforderungen an Datenschutzbeauftragte.

DSGVO (Datenschutz-Grundverordnung der EU)

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die den Schutz personenbezogener Daten innerhalb der Europäischen Union (EU) und des Europäischen

[31] (ChatGPT, kein Datum)

Wirtschaftsraums (EWR) regelt. Sie legt strenge Regeln für die Erhebung, Speicherung, Verarbeitung und den Schutz personenbezogener Daten fest. Die DSGVO hat extraterritoriale Auswirkungen und betrifft Unternehmen außerhalb der EU, die Daten von EU-Bürgern verarbeiten.

Swiss-US Privacy Shield

Das Swiss-US Privacy Shield war ein Rahmenwerk für den transatlantischen Datentransfer zwischen der Schweiz und den USA. Es wurde 2017 geschaffen, um Unternehmen in beiden Ländern eine Methode zur Einhaltung der Datenschutzbestimmungen zu bieten, indem es Datenschutzprinzipien für den Datentransfer festlegte. Allerdings wurde das Privacy Shield 2020 vom Schweizer Datenschutz- und Öffentlichkeitsbeauftragten offiziell aufgehoben.

EU-US Privacy Shield

Ähnlich wie das Swiss-US Privacy Shield war das EU-US Privacy Shield ein Rahmenwerk für den transatlantischen Datentransfer zwischen der EU und den USA. Es sollte gewährleisten, dass Unternehmen, die Daten zwischen diesen Regionen übertragen, dies unter Einhaltung der Datenschutzstandards tun. Das EU-US Privacy Shield wurde jedoch ebenfalls 2020 vom Europäischen Gerichtshof für ungültig erklärt.

Cloud Act (Clarifying Lawful Overseas Use of Data Act)

Der Cloud Act ist ein US-amerikanisches Gesetz, das 2018 verabschiedet wurde und die Freigabe von Daten in der Cloud regelt. Es erlaubt US-Behörden den Zugriff auf Daten, die von US-Technologieunternehmen außerhalb der USA gespeichert werden. Das Gesetz hat Auswirkungen auf Cloud-Service-Anbieter und den Zugriff auf Daten, die außerhalb der USA gespeichert sind, was Bedenken hinsichtlich des Datenschutzes und der Privatsphäre aufwirft.

Unternehmen und Organisationen, die in diesen Regionen tätig sind oder personenbezogene Daten von Personen in diesen Regionen verarbeiten, müssen die jeweiligen Datenschutzbestimmungen und -anforderungen beachten.[32]

Kennt die Problematik von Datenlöschungen über alle Archive und Backups.

Daten sind in der heutigen digitalen Welt verschiedenen Gefahren ausgesetzt. Hier sind einige der häufigsten Gefahren, denen Daten ausgesetzt sein können:

1. **Diebstahl:** Daten können gestohlen werden, sei es physisch durch den Diebstahl von Geräten wie Laptops oder Servern oder digital durch unbefugten Zugriff auf Computersysteme oder Netzwerke.
2. **Ransomware:** Ransomware ist eine Art von Schadsoftware, die Daten verschlüsselt und Lösegeld von den Opfern verlangt, um die Daten wiederherzustellen. Wenn das Lösegeld nicht gezahlt wird, können die Daten verloren gehen.
3. **Malware:** Malware (schädliche Software) kann dazu verwendet werden, Daten zu stehlen, zu beschädigen oder zu manipulieren. Dies kann Spyware, Viren, Würmer und Trojaner umfassen.
4. **Phishing:** Bei Phishing-Angriffen werden gefälschte E-Mails oder Websites verwendet, um Benutzer zur Preisgabe sensibler Daten wie Benutzernamen und Passwörtern zu verleiten.
5. **Hacking und unbefugter Zugriff:** Angreifer können versuchen, sich unbefugten Zugriff auf Computersysteme, Netzwerke oder Online-Konten zu verschaffen, um Daten zu stehlen oder zu manipulieren.

[32] (ChatGPT, kein Datum)

6. **Social Engineering:** Bei dieser Methode manipulieren Angreifer Menschen, um vertrauliche Informationen preiszugeben. Dies kann durch Täuschung, Betrug oder Manipulation erfolgen.
7. **Datenlecks:** Datenlecks können durch menschliche Fehler oder Schwachstellen in Systemen verursacht werden. Infolge von Datenlecks werden vertrauliche Informationen versehentlich oder absichtlich veröffentlicht.
8. **Physische Schäden:** Daten können durch Naturkatastrophen wie Überschwemmungen, Brände oder Erdbeben gefährdet sein, wenn die physische Infrastruktur beschädigt wird.
9. **Integritätsverletzungen:** Eine Integritätsverletzung tritt auf, wenn Daten absichtlich oder unbeabsichtigt geändert werden, was zu Datenkorruption oder Manipulation führt.
10. **Datenverlust:** Daten können aufgrund von technischen Ausfällen, Hardwareproblemen oder versehentlicher Löschung verloren gehen.
11. **Datenspeicherprobleme:** Probleme mit Datenspeichergeräten, wie Festplatten oder SSDs, können zum Verlust oder zur Beschädigung von Daten führen.
12. **Wirtschaftsspionage:** In diesem Fall versuchen Angreifer, sensible Unternehmensdaten oder geistiges Eigentum zu stehlen, um Wettbewerbsvorteile zu erlangen.
13. **Rechtliche und Compliance-Risiken:** Unternehmen und Organisationen müssen Daten nach geltenden Gesetzen und Vorschriften schützen, da Verstöße zu rechtlichen Konsequenzen führen können.

Um Daten effektiv zu schützen, ist es wichtig, Sicherheitsmaßnahmen wie Verschlüsselung, regelmäßige Datensicherungen, Firewalls, Antivirensoftware, Schulungen zur Sensibilisierung der Benutzer und Sicherheitsrichtlinien zu implementieren. Datenschutz und Datensicherheit sind entscheidend, um Daten vor den oben genannten Gefahren zu schützen.[33]

Kennt wesentliche juristische Voraussetzungen und Eigenheiten von Websites (z. B. Impressum, Disclaimer, AGBs).

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?

AGB

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.

[33] (ChatGPT, kein Datum)

- 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).

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
- Mehrwertsteuernummer (falls vorhanden)
- UID oder Handelsregisternummer (falls vorhanden)
- Allfällige Aufsichtsbehörden (falls vorhanden)

Es gibt verschiedene Online-Dienste und Tools, die Ihnen bei der Erstellung und Überprüfung rechtlicher Dokumente wie Allgemeiner Geschäftsbedingungen (AGB) helfen können.[34]

(Kennt verschiedene Lizenzmodelle (z. B. für Software, Texte, Bilder))

Verschiedene Lizenzmodelle werden für die Bereitstellung von Software, Texten, Bildern und anderen kreativen Werken verwendet. Hier sind einige der gängigsten Lizenzmodelle:

1. Proprietäre Lizenz (Closed Source):

- Dies ist das traditionelle Modell, bei dem die Urheberrechte für die Software oder das Werk vollständig bei den Erstellern oder Rechteinhabern liegen. Die Nutzung und Verteilung ist eingeschränkt und erfordert oft den Kauf oder eine Lizenzierung.

2. Open-Source-Lizenz:

- Bei Open-Source-Software werden die Quellcodes öffentlich zugänglich gemacht, und die Software kann von jedem genutzt, modifiziert und weiterverbreitet werden. Es gibt verschiedene Open-Source-Lizenzen, darunter die GNU General Public License (GPL), die Apache License und die MIT License.

3. Freie Software-Lizenz:

- Ähnlich wie Open Source, aber betont die Freiheit der Benutzer, die Software zu verwenden, zu kopieren, zu ändern und zu verbreiten. Die Free Software Foundation (FSF) definiert Richtlinien, die von Lizenzen wie der GNU GPL eingehalten werden.

4. Creative Commons-Lizenz:

- Dieses Lizenzmodell wird für kreative Werke wie Texte, Bilder und Musik verwendet. Es erlaubt den Urhebern, bestimmte Nutzungsrechte zu gewähren, während andere

[34] (OneNote Modul 231, kein Datum)(231-3A Evaluation)

eingeschränkt bleiben. Es gibt verschiedene Arten von Creative Commons-Lizenzen, darunter Attribution (BY), Share-Alike (SA), Non-Commercial (NC) und No Derivatives (ND).

5. Proprietäre Software-Lizenz:

- Software-Unternehmen verwenden verschiedene Arten von proprietären Lizenzen, um die Verwendung und Verteilung ihrer Software zu regulieren. Beispiele sind Endbenutzer-Lizenzverträge (EULAs), die oft mit Software-Anwendungen gebündelt sind.

6. GNU General Public License (GPL):

- Dies ist eine Open-Source-Lizenz, die die Freiheit der Benutzer betont, Software zu verwenden, zu modifizieren und weiterzugeben. Die GPL hat verschiedene Versionen, darunter die GPLv2 und die GPLv3.

7. Apache License:

- Diese Open-Source-Lizenz wird häufig für Softwareprojekte im Zusammenhang mit Webtechnologien und Server-Software verwendet.

8. MIT License:

- Die MIT License ist eine einfache und weit verbreitete Open-Source-Lizenz, die es erlaubt, Software frei zu verwenden, zu modifizieren und weiterzugeben, solange der Urheberrechtsvermerk beibehalten wird.

9. Public Domain (Gemeinfreiheit):

- Werke, die in die Gemeinfreiheit gestellt werden, haben keine urheberrechtlichen Beschränkungen und können von jedermann frei genutzt werden.

10. Copyleft-Lizenz: - Copyleft-Lizenzen, wie die GPL, verlangen, dass modifizierte Versionen des Werks ebenfalls unter denselben Bedingungen veröffentlicht werden, um sicherzustellen, dass die Freiheit der Benutzer erhalten bleibt.

Diese Lizenzmodelle dienen dazu, die Verwendung und Verbreitung von Software, Texten, Bildern und anderen Werken zu regeln und sicherzustellen, dass die Rechte und Freiheiten der Ersteller und Nutzer respektiert werden. Die Wahl des richtigen Lizenzmodells hängt von den Zielen und Anforderungen der Urheber und Nutzer ab.[35]

Übungsaufgaben

231-1A - 00 Einführung in den Datenschutz

231-1B - 00 Passwörter

231-2A - 00 Authentisierung, Authentifizierung und Autorisierung

231-2B - 00 IT-Sicherheitskonzept

231-2C - 00 Datenschutz einer Homepage (DSGVO-konform)

231-3A - 00 Datenschutz einer Homepage (Datenschutzerklärung, AGB, Impressum)

231-3B - 00 CMS-System

[35] (ChatGPT, kein Datum)

231-3C - 00 Cookies

231-4A - 00 Personenbezogene Daten

231-4B - 00 Schutzziele

231-5A - 00 Backup und Archivierung

231-5B - 00 Datenschutz beim Fallbeispiel Whatsapp

231-6A - 00 Datenschutz beim Fallbeispiel Steam

231-7A - 00 Datenschutz gewährleisten, Datenschutz technische Massnahmen

231-8A - 00 Webstore erstellen, was gilt zu beachten