Weshalb schütze ich meine Daten?

Einzelauftrag „Mind-Map“ (Zeitaufwand total 60 Minuten):

Durchlesen **15 Min.**

Lesen Sie den Auftrag und den Fachtext zuerst in Ruhe durch. Beginnen Sie anschliessend, wichtige Textpassagen zu markieren. Dabei können Sie sich überlegen, wie sie die aussagekräftigsten Inhalte in einem Mindmap zusammenfassen können. Eine passende Möglichkeit dazu wäre, für die entsprechenden Kapitel und Unterkapitel jeweils eigene Äste und Unteräste zu zeichnen.

Mindmap

Vorbereitung / gut zu wissen:

A4-Blatt (bei der Lehrperson beziehen) oder ein Mindmap-Tool verwenden (zum Beispiel mindmup.com).

1. A4-Blatt (Skizze, Draft) ← darauf skizzieren Sie ihre Ideen und Ihren Entwurf
2. Diese Zusammenfassung können Sie bei der später folgenden LB1 als „Spick“ verwenden

Bearbeitung Skizze **30 Min.**

Beginnen Sie mit der Skizze / Zusammenfassung

3. Benutzen Sie dazu vorzugsweise Bleistift und Radiergummi
4. Versuchen Sie anhand einer für Sie verständlichen Skizze (z.B Baum) den Textinhalt zu visualisieren. Eine Möglichkeit wäre z.B. die einzelnen Kapitel und Unterkapitel als Stämme und Äste darzustellen und anschliessen mit wichtigen Stichworten anzuschreiben.

Falls die Zeit ausreicht, übertragen sie ihre Skizzen auf ein neues A4-Blatt (evtl. Hausaufgabe) **15 Min.**

Mit dieser Übung vertiefen sie ihr Verständnis – gleichzeitig können sie Inhalte und Struktur des ersten Drafts ausbessern – möglichst so, dass sie ihre Notizen bei der später folgenden Lernkontrolle besser anwenden können

5. Nehmen Sie Marker und verschiedene Farben zur Hilfe.
6. Nutzen Sie den verfügbaren Platz aus
7. Zeigen Sie das Dokument nach Abschluss der Lehrperson. Sobald dieses visiert ist, kann es als Spick für die folgende Lernkontrollen (LB1) verwendet werden.

Falls Sie mindmup verwenden: Link speichern, Mindmup downloaden als mindmup-File

Folgeauftrag (Hausaufgaben)

Erstellen Sie ein Dokument, welches die vier unten gestellten Fragen – und ihre persönlichen Antworten beinhaltet. Abgabe: BSCW (Gem. Angaben der Lehrperson) Beachten Sie den **Abgabetermin** und die **Bezeichnung**.

1. In welche drei Ursachen werden Bedrohungen eingeteilt?
2. Was ist mit Eintrittswahrscheinlichkeit eines Risikso gemeint? Wie hoch schätzen sie die Möglichkeit ein, dass ein Virus Daten auf ihrem System zerstört? Treffen sie Massnahmen? Wie gehen sie dabei vor? (Erklären sie in Stichworten)
3. Was regelt der Datenschutz? Was bedeuten diese Regelungen für die verantworlichen Informatiker?
4. Welche Unterschiede zwischen Backup und Archivierung können sie aufzählen? Kennen sie Gründe die für die eine oder andere Methode sprechen? Welche würden sie für ihre persönlichen Daten auswählen?

Bedrohungsarten

Bedrohungen im ICT-Umfeld haben verschiedene Ursachen. Grundsätzlich werden diese in drei Hauptgruppen aufgeteilt.

Höhere Gewalt	Kriminelle Handlungen	Menschliches Versagen
		
• Erdbeben	• Diebstahl	• Versehentliches Löschen von Daten
• Blitzschlag	• Hacking, Spionage	• Fehlerhaftes Programmieren
• Feuer, Explosion	• Viren, Malware	• Falsche Anweisungen
• Defekte Hardware	• Sabotage	• Falsche Berechtigungen

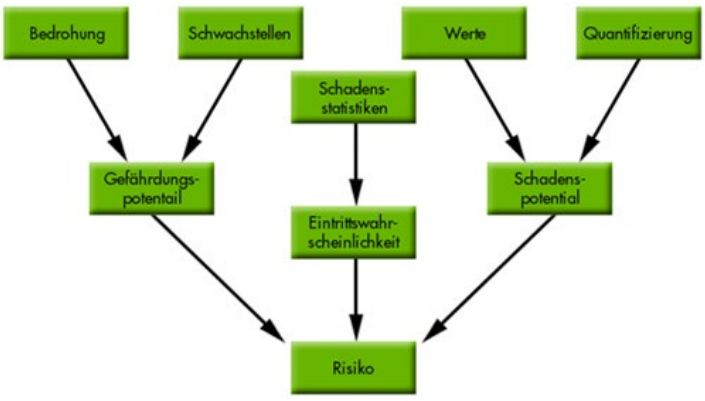
Schutzmassnahmen

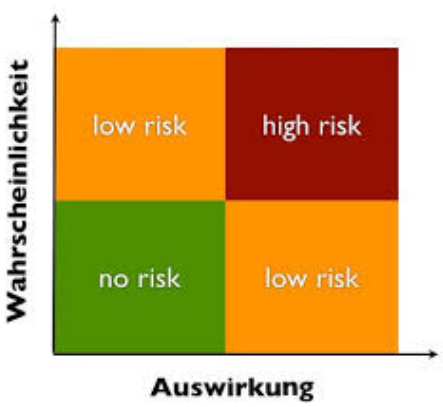
In der Informatik gibt es zahlreiche und vielfältige Präventivmassnahmen, um den unterschiedlichsten Bedrohungen gerecht zu werden. Diese werden in folgende drei Kriterien unterteilt:

Technische Massnahmen	Bauliche Massnahmen	Organisatorische Massnahmen
• Backup	• Alarmanlage	• Prozesse einführen
• Antivirenprogramme	• Erdbebensicher	• Verantwortlichkeit def.
• Datenverschlüsselung	• Zugangskontrolle	• Schulung

Risikoanalyse

Anhand einer Risikoanalyse werden die Gefahren in einem ersten Schritt eingestuft und bewertet.





Schrittfolge der Risikoanalyse

Schritt 1:

Definition eines systematischen Ansatzes für den Umgang mit Risiken (Risikomanagement)

Schritt 2:

Beschreibung und Erläuterung eines geeigneten Ansatzes (Methode) zur Analyse, Bewertung und Behandlung von Informationssicherheit Risiken (Risikomanagementhandbuch): Festlegung der Schutzklassen und Kriterien (Schadenshöhe, Eintrittswahrscheinlichkeit, Risikoakzeptanz), Bestimmung der Verantwortlichkeiten, Definition der Review-Zyklen

Schritt 3:

Prozessbeschreibung zum IT Risikomanagement

Schritt 4:

Erfassen aller (potenziell) **bedrohten Objekte und deren Wert** (Klassifizieren nach Schutzklassen)

Schritt 5:

Erfassen der Daten und Informationen (Klassifizieren nach Schutzklassen) durch eine IT Risikoanalyse

Schritt 6:

Erfassen der Bedrohungen und der Schwachstellen im IT Bereich. Dabei sollte man folgende Dinge beachten: Die Bedrohungen sind im Zuge der Risikoanalyse im IT Bereich in einer Excel Tabelle systematisch zu dokumentieren, möglichen Schäden durch Verlust, Veränderung oder Ausfall zu bewerten und die Schäden in einer Excel Tabelle systematisch zu dokumentieren und zu bewerten.

Schritt 7:

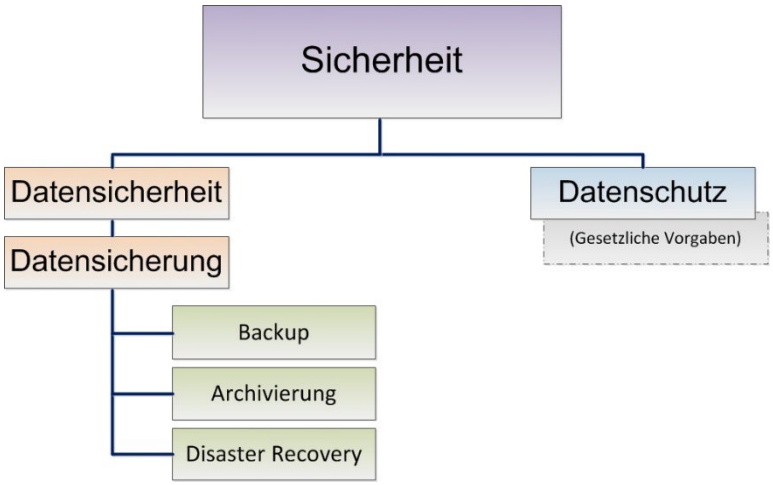
Bewertung der Eintrittswahrscheinlichkeit eines IT Risikos

Schritt 8:

Erstellung einer Risikomatrix (siehe Grafik)
Diese bringt die Eintrittswahrscheinlichkeit pro Schaden, sowie die zu erwartende Schadenshöhe miteinander in Bezug.

Einordnung der Begriffe «Backup» und «Restore»

In diesem Abschnitt ordnen wir die Begriffe, um Klarheit zu schaffen, weshalb das Thema «Datensicherheit» in der Informatik so wichtig ist. Ausserdem lernen sie den Unterschied zwischen «Datenschutz und Datensicherheit» kennen



Defintion von Datenschutz

Beim Datenschutz handelt es sich um **personenbezogene Daten** und deren Schutz vor Missbrauch während **Erhebung**, **Verarbeitung** und **Nutzung**. Dabei soll das Recht auf informationelle Selbstbestimmung gewährt bleiben, wodurch jeder Mensch nach dem Schweizerischen Datenschutzgesetz frei und selbst darüber entscheiden kann wie mit seinen persönlichen Daten umgegangen wird, sofern kein Gesetz eine andere Regelung vorsieht.

Definition: personenbezogene Daten

Dies sind Einzelangaben über persönliche Verhältnisse (z.B. über Kinder, Familie, Krankheiten, Interessen) oder sachliche Verhältnisse (z.B. Kontodaten, Versicherungen, Einkommen) welche einer bestimmten natürlichen Person (z.B. Josef Meier geboren am 28.2.1987 in Zürich) oder einer bestimmbaren natürlichen Person (z.B. Herr Müller wohnhaft im Erlenweg 12 in Meilen) zugeordnet werden können. Die so bestimmte oder bestimmbare Person wird im Gesetz auch als “Betroffener” bezeichnet.

Definition von Datensicherheit

Unter Datensicherheit wird der Schutz von Daten vor Verlust, Verfälschung, Beschädigung oder Löschung durch Maßnahmen und durch Software verstanden. Datensicherheit ist essentieller Bestandteil der gesamten Informationssicherheit und dient auch zur Vermeidung und Bekämpfung von Cyberkriminalität

Ziele der Datensicherheit

Vertraulichkeit	Nur berechtigte Personen dürfen Zugriff auf diese Informationen haben
Integrität	Daten dürfen nicht unbemerkt verändert werden
Verfügbarkeit	Der Zugriff auf die Daten muss gewährleistet sein
Authentizität	Echtheit und Vertrauenswürdigkeit der Daten muss gewährleistet sein

Datenschutz ist **nicht** Datensicherheit!

«Datenschutz» meint den Schutz von personenbezogenen Daten, wie z. B. Name, Adresse, Geburtsdatum, E-Mail-Adresse, Telefonnummer usw. Er obliegt in erster Hinsicht dem Besitzer der Daten. Jede und Jeder muss selbst entscheiden, welche persönlichen Daten sie oder er an Dritte (auch z. B. Social Media: Facebook, Twitter, Google+) weitergibt.

Weshalb benötigen wir Datensicherungen?

Bösartige Computer-Viren können zu Datenverlust führen, indem sie Dateien auf Ihrem Computer löschen oder verändern. Auch eindringende Hacker können Daten verändern, löschen oder missbrauchen.

In den meisten Fällen führt jedoch das Fehlverhalten des Anwenders zu Datenverlust: Eine Datei, die eigentlich noch benötigt würde, wird versehentlich gelöscht. Nicht zu unterschätzen sind auch Fehler, die in täglich verwendeter Software auftreten können.

Bei Hardwarefehlern handelt es sich oft um eine altersbedingte Schädigung an der Schreib- und Lesevorrichtung der Platte. Der regelmässige Gebrauch führt aber auch zu Abnützungen sämtlicher elektronischen Komponenten (Temperaturschwankungen, Transport etc…) und führt mit der Zeit dazu, dass elektronische Komponenten ausfallen können. Sind diese nicht redundant ausgelegt, kann es so schnell zu einem Ausfall des Systems – und demzufolge zu Datenverlust kommen.

Backup vs. Archivierung

Innerhalb der Datensicherung werden die Begriffe «Backup» und «Archivierung» unterschieden. Grundsätzlich haben diese beiden Begriffe einige Gemeinsamkeiten. Hard- und Software können unter Umständen gleich oder ähnlich. Dennoch gibt es ein paar wichtige Erkenntnisse, die bei der Entwicklng eines Datensicherungs-Konzeptes berücksichtigt werden sollten.

Backup

Primäres Ziel: Datenverlust vermeiden.
Beim Herstellen eines Backups wird zu einem bestimmten Zeitpunkt ein Duplikat von Daten erstellt, auf das zurückgegriffen werden kann. Die Daten im Quellverzeichnis bleiben demzufolge bestehen.

Archivierung

Primäres Ziel: Daten gem. gesetzlichen oder vertraglichen Vorgaben aufbewahren.
Archivdaten werden in der Regel auf ein separates Medium geschrieben und aus platzgründen vom ursprünglichen Laufwerk (Quelle) gelöscht.

Beim Archiv gelten folgende Aspekte:

- Gesetzlich vorgeschrieben
- Nachvollziehbarkeit der Geschäftsvorfälle, Beweismittel
- Kosten- und Platzeinsparung durch Auslagerung

	Backup	Archiv
Ziel	Wiederherstellung von gelöschten oder zerstörten Daten	Geschäftsdaten (z.B. Bilanz) nach gesetzlichen oder vertraglichen Vorgaben aufbewahren
Dauer	Kurz- bis mittelfristig. Wenige Wochen bis einige Monate	Langfristig: Mehrere Jahre (je nach gesetlichen oder vertraglichen Vereinbarungen
Originaldaten	Daten werden kopiert (und bleiben in der Regel auf dem Originalsystem)	Daten werden verschoben (und in der Regel auf dem Originalsystem gelöscht)

Restore

Gesicherte Daten werden zurückgespielt (wiederhergestellt). Die Umkehrung des Backup- oder Archivierungsvorganges.

Disaster Recovery

Nomen est omen. Grössere Firmen bauen zur Sicherheit oftmals ein zweites Rechenzentrum an einer anderen geografischen Lage. Trifft der Fall ein, dass ein Serverraum komplett ausfällt (Erdbeben, Überflutung etc…) müssen die Kern-Applikationen möglichst nahtlos und ohne Datenverlust am Leben erhalten bleiben - oderwieder zum Laufen gebracht werden. Für solche Fälle entwickeln ICT-Fachleute entsprechende Notfallszenarien, welche auch regelmässig in vorgegebenen Zeitintervallen zu testzwecken (als Trockenübung) trainiert werden. Ein Disaster-Recovery-Plan sieht **nicht** vor, dass der Betrieb im Ursprungsrechenzentrum wieder hergestellt werden kann – man geht also davon aus, dass die betroffene «Site» komplett zerstört sein kann und deshalb zuerst wieder neu aufgebaut werden muss. Die Wahrscheinlichkeit, dass ein solches Ereignis eintritt ist sehr gering – deshalb ist es umso wichtiger, dass dieser Prozes aktuell gehalten wird und zuverlässig dokumentiert ist