1 Warum müssen Daten gesichert werden?

Und plötzlich ist alles schwarz. Der Computer hat sich verabschiedet, die Daten sind nicht mehr zu retten. Ein Albtraum sowohl in der Geschäftswelt als auch im Privatleben. Der Computer ist rasch ersetzt. Kosten doch die Geräte heutzutage nicht mehr alle Welt. Aber was ist mit den Daten?

1.1 Wert der Unternehmensdaten

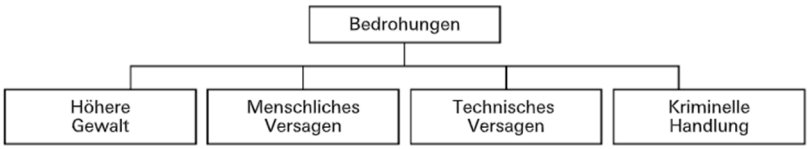
In der Geschäftswelt werden praktisch alle Vorgänge auf dem Computer erfasst, bearbeitet und gespeichert. Schnell sind so grosse Datenmengen vorhanden. Doch wie hoch ist der Wert dieser Daten? Sind noch Dokumente auf Papier vorhanden, können die Informationen nachträglich manuell wieder eingegeben werden. Der Aufwand hierfür kann genau berechnet und ausgewiesen werden. Doch wie berechnen Sie die Kosten für Daten, die Sie nicht mehr rekonstruieren können?

Stellen Sie sich vor, Ihre Hausbank verliert aus Versehen Kontodaten. Ihr Vermögen und das anderer Kunden ist plötzlich nicht mehr auffindbar. Sicherlich würden Sie nicht lange überlegen, Ihr Konto bei dieser Bank aufzulösen (was Sie ja aufgrund der Situation nicht einmal mehr machen müssten). Mit anderen Worten kann die Existenz eines Unternehmens von der sicheren Aufbewahrung und Rekonstruierbarkeit seiner Daten abhängen. Daten können daher unbezahlbar sein.

1.2 Bedrohungen der Unternehmensdaten

Die Werte in der ICT unterliegen einer ständigen Bedrohung. Diese Bedrohungen können verschiedene Ursachen haben. Nachfolgend werden die vier wesentlichen Ursachen von Bedrohungen vorgestellt.

[1-1] Gefahrenkategorien



1.2.1 Höhere Gewalt

Bei der höheren Gewalt kommt die Bedrohung von aussen. Unternehmen haben auf diese Ereignisse meistens keinen Einfluss. Zu diesen Ereignissen werden nachfolgende Risiken gerechnet:

- Feuer, Explosion im Rechenzentrum oder in dessen Umgebung
- Naturkatastrophen wie Erdbeben, Überschwemmung oder Blitzschlag
- Stromausfall

1.2.2 Menschliches Versagen

Die Mehrheit der Zwischenfälle lässt sich auf menschliches Versagen zurückführen. Darunter gehören nachfolgende Risiken:

- Versehentliches Löschen von Daten
- Fehlerhaftes Programmieren
- Verlust der Vertraulichkeit durch herumliegende Daten
- Fehlende Dokumentation

1.2.3 Technisches Versagen

Beim technischen Versagen fallen technische Geräte wegen eines Defekts aus. Mögliche Gründe können wie folgt sein:

- Hardwaredefekt
- Softwarefehler
- Defekte an Systemen
- Defekte an Netzwerkkomponenten

1.2.4 Kriminelle Handlung

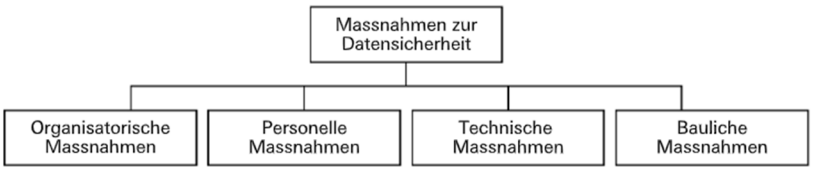
Im Gegensatz zum menschlichen Versagen löschen bzw. zerstören die Menschen Daten nicht unabsichtlich, sondern gewollt. Unter kriminellen Handlungen werden nachfolgende Risiken verstanden:

- Absichtliche Manipulation an Geräten, Programmen oder Daten
- Missbrauch vertraulicher Daten
- Diebstahl oder Kidnapping von Geräten, Programmen oder Daten
- Einbringen von bösartiger Software (Viren)
- Hacking, Industriespionage
- Vandalismus
- Sabotage

1.3 Massnahmen zur Datensicherheit

Durch gezielte Risikoanalyse von bestimmten Objekten werden unmittelbare Bedrohungen erkannt und abgeschwächt bzw. eliminiert. Diese Massnahmen lassen sich in organisatorische, personelle, technische und bauliche Massnahmen unterteilen.

[1-2] Massnahmenkategorien



1.3.1 Organisatorische Massnahmen

Bei den organisatorischen Massnahmen wird die Organisation des Unternehmens angepasst. Unter Organisation werden der Aufbau (z. B. das Organigramm) oder die Prozesse verstanden. Es fallen aber auch die Informationen an die Mitarbeitenden, z. B. mittels Weisung oder Schulung, darunter. Mögliche organisatorische Massnahmen sind:

- Dokumentation des Sicherheitskonzepts
- Herausgabe von Verhaltensweisungen
- Optimierung von Sicherheitsabläufen
- Erstellung von Arbeitsbeschreibungen
- Schulung der Anwender bzw. Benutzer

1.3.2 Personelle Massnahmen

Personelle Massnahmen umfassen Massnahmen, bei denen das Personal, also die Mitarbeitenden, direkt betroffen sind. Mögliche personelle Massnahmen sind:

- Einstellen eines Sicherheitsverantwortlichen
- Zuteilung von Mitarbeitenden in andere Abteilungen bzw. Funktionen
- Entlassung von Mitarbeitenden, z. B. nach krimineller Aktivität

1.3.3 Technische Massnahmen

Hier wird die Datensicherheit mithilfe technischer Massnahmen im ICT-System sichergestellt. Mögliche technische Massnahmen sind:

- Datensicherung (Backup & Restore)
- Anmeldung durch Passwort
- Verschlüsselung von Daten
- Firewall
- Antivirenprogramme

▷ **Hinweis**

Wie Sie sehen, ist das Backup & Restore eine technische Massnahme zur Datensicherung. Die Datensicherung wiederum ist ein Teilbereich der Datensicherheit.

1.3.4 Bauliche Massnahmen

Bei den baulichen Massnahmen wird die Datensicherheit mittels Umbau der Infrastruktur gewährleistet. Mögliche bauliche Massnahmen sind:

- Blitzschutz einbauen
- Feuerschutz installieren
- Einbruchsschutz einbauen
- Alarmanlage installieren

1.4 Preloss oder Postloss

Massnahmen dienen einerseits dazu, Bedrohungen vor dem Entstehen bereits zu eliminieren **(Preloss)**. Andererseits können Massnahmen auch dazu dienen, im Falle eines Ereignisses die Weiterführung zu gewährleisten **(Postloss)**.

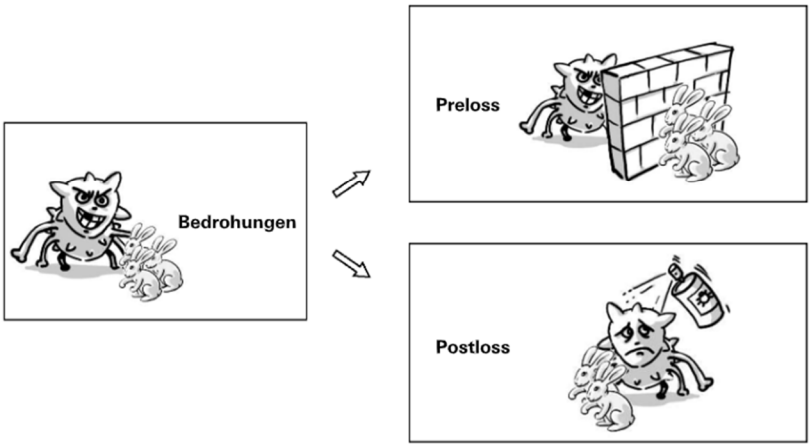
Preloss	Postloss
Dies sind Massnahmen, die die Eintrittswahrscheinlichkeit eines Ereignisses verhindern sollen. Es sind also präventive Massnahmen zur Reduktion der Eintrittswahrscheinlichkeit einer Bedrohung.	Dies sind Massnahmen, die zur Schadensbegrenzung beitragen. Es sind also restriktive Massnahmen zur Begrenzung der Schadengrösse.

Beispiel

Beim Auto wird ein ABS installiert, damit der Fahrer auch in schwierigen Lagen sein Auto steuern kann. Unfälle können so verhindert werden. Das ABS stellt eine Preloss-Massnahme dar. Die Unfallabteilung in einem Spital ist eine Postloss-Institution. Sie versucht, den Schaden zu begrenzen. Damit im Falle eines Unfalls die Kosten gedeckt sind, werden Unfallversicherungen abgeschlossen. Bei der Versicherung handelt es sich um eine finanzielle Postloss-Massnahme. Sie verhindert keinen Schaden, sondern nur die finanziellen Auswirkungen.

Das in diesem Lehrmittel behandelte Thema «Datensicherung» ist eine Massnahme im Bereich Postloss. Eine Datensicherung dient dazu, bereits gelöschte bzw. zerstörte Daten wiederherstellen zu können.

[1-3] Preloss oder Postloss



1.5 Betriebliche Rahmenbedingungen

Praktisch alle Geschäftsprozesse starten mit der Aufnahme von Daten und enden mit dessen Speicherung. Ein Ausfall der Systeme und somit das Wegfallen der Datenverarbeitung zieht den Stillstand des Unternehmens mit sich. Datensicherheit ist gegeben, wenn die folgenden drei Grundwerte eingehalten werden:

[1-4] Grundwerte der Datensicherheit

1.5.1 Vertraulichkeit

Die Daten werden unter Einhaltung des Datenschutzgesetzes (siehe Kap. 1.6.2, S.16) bearbeitet. Mit geeigneten Massnahmen wird verhindert, dass unberechtigte Personen Zugriff auf nicht für sie bestimmte Daten haben, beispielsweise durch Verschlüsselung der Daten.

1.5.2 Integrität

Unter Integrität wird die Korrektheit und Vollständigkeit von Informationen und Daten verstanden. Beispielsweise die korrekte Schreibweise der Nachnamen der Kunden. Zudem sind die Daten frei von Manipulation.

1.5.3 Verfügbarkeit

Ein System muss immer dann verfügbar sein, wenn der Benutzer damit arbeiten möchte. Natürlich gelten hier die Regelungen zur Wartung der Systeme zwischen Anbieter der Systeme und dem Benutzer. So wird z. B. abgemacht, dass die Computer während den Bürozeiten 99.9% zur Verfügung stehen.

1.6 Gesetzliche Vorschriften

Der Schutz der Daten ist ebenfalls gesetzlich vorgeschrieben. In der Schweiz sind in Bezug auf Datensicherheit v. a. das Obligationenrecht (OR) sowie das Datenschutzgesetz (DSG) relevant.

1.6.1 Obligationenrecht (OR)

Jedes Unternehmen ist gesetzlich dazu verpflichtet, seine Daten auf bestimmte Zeit, i. d. R. 10 Jahre, aufzubewahren. Diese Daten können auf Papier oder elektronisch gesichert werden. Das Unternehmen hat also Sorge zu tragen, dass Ihre Daten während der gesetzlich vorgeschriebenen Zeit aufbewahrt werden und während dieser Zeit jederzeit gelesen werden können. Die dazugehörige GeBüV von 2002 regelt die Grundsätze für eine ordnungsgemässe Aufbewahrung sowie die zulässigen Datenträger im Detail.

1.6.2 Datenschutzgesetz (DSG)

Daten über natürliche und juristische Personen sind sensibel und müssen daher geschützt werden. Sie wären bestimmt auch nicht erfreut, wenn jeder Ihre Krankenakte oder Ihre Lohndaten einsehen könnte. Der Umgang mit Personendaten ist im **Datenschutzgesetz (DSG)** geregelt. Das Schweizer Datenschutzgesetz will in erster Linie die Persönlichkeit und die Grundrechte von Personen schützen, über die Daten bearbeitet werden. **Besonders schützenswert** sind gemäss Art. 3 Abs. c DSG folgende Personendaten:

- Religiöse Ansichten, z. B. Zugehörigkeit zu einer Landeskirche
- Weltanschauliche Ansichten
- Politische Ansichten und Tätigkeiten
- Gesundheit, z. B. der Blutwert eines Patienten
- Intimsphäre
- Rassenzugehörigkeit

Sobald ein Unternehmen Personendaten speichert und bearbeitet, muss dem Datenschutz besondere Beachtung geschenkt werden. Gemäss Art. 7 DSG müssen angemessene technische und organisatorische Massnahmen getroffen werden, um solche Daten gegenüber unbefugter Bearbeitung zu schützen. Für die Planung und Umsetzung geeigneter Schutzmassnahmen bietet die **Verordnung zum Datenschutzgesetz (VDSG)** eine Hilfestellung. In Art. 9 VSDG[1] heisst es unter anderem:

«Der Inhaber der Datensammlung trifft insbesondere bei der automatisierten Bearbeitung von Personendaten die technischen und organisatorischen Massnahmen, die geeignet sind, namentlich folgenden Zielen gerecht zu werden:

a. Zugangskontrolle: unbefugten Personen ist der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren;

b. Personendatenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen;

c. Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können;

d. Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können;

e. Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern;

f. Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern;

g. Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen;

h. Eingabekontrolle: in automatisierten Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden.»