Der Wert von Informationen

1.2.1 Grundlegende Merkmale der Datensicherheit verstehen: Vertraulichkeit, Integrität, Verfügbarkeit

Um Daten zu schützen und zuverlässig nutzen zu können, sind drei zentrale Sicherheitsmerkmale entscheidend: Vertraulichkeit, Integrität und Verfügbarkeit.

- **Vertraulichkeit:** Vertraulichkeit bedeutet, dass nur berechtigte Personen auf bestimmte Informationen zugreifen können. Sensible Daten sollen vor unbefugtem Zugriff geschützt sein.

Beispiel: In einem Unternehmen können Gehaltsdaten nur von autorisierten Mitarbeitern in der Personalabteilung eingesehen werden, nicht jedoch von anderen Kollegen.

Integrität: Integrität bedeutet, dass die Daten korrekt, vollständig und unverändert sind. Dies umfasst verschiedene Aspekte:

- **Inhaltliche Korrektheit:** Daten müssen frei von Manipulation sein und dem Original entsprechen. Werden Informationen verändert, müssen diese Änderungen nachvollziehbar und dokumentiert sein.
- **Temporale Korrektheit:** Die Aktualität der Daten muss gewährleistet sein, damit Entscheidungen auf der Grundlage der richtigen Informationen getroffen werden. Veraltete oder verspätete Daten können zu falschen Schlussfolgerungen führen.
- **Konsistenz und Vollständigkeit:** Daten sollten fehlerfrei und vollständig sein. Wenn wichtige Informationen fehlen oder inkonsistent sind, ist die Aussagekraft der Daten eingeschränkt.

Beispiel zur Datenintegrität: In einem Krankenhaus müssen Patienteninformationen aktuell und korrekt sein. Falsche oder veraltete Informationen, wie eine nicht mehr gültige Medikamentenliste, könnten zu schweren Behandlungsfehlern führen.

Verfügbarkeit: Verfügbarkeit bedeutet, dass Daten und Systeme dann zugänglich sind, wenn sie gebraucht werden. Dies umfasst die Uptime, also die Zeit, in der Systeme betriebsbereit sind. Ein Ausfall oder eine Sperrung wichtiger Daten kann den Betrieb erheblich beeinträchtigen.

Beispiel: Für einen Notfallarzt ist es entscheidend, jederzeit auf Patientendaten zugreifen zu können. Ein Ausfall des Datenzugangs könnte lebensbedrohliche Konsequenzen haben. Unternehmen streben in der Regel eine Uptime von 99,9 % oder mehr an, um sicherzustellen, dass Systeme stets verfügbar sind.

1.2.2 Warum personenbezogene Daten zu schützen sind

Personenbezogene Daten sind Informationen, die sich direkt oder indirekt auf eine Person beziehen, wie Name, Adresse, Kontaktdaten oder persönliche Gesundheitsdaten. Der Schutz dieser Daten ist besonders wichtig, um die Privatsphäre der Menschen zu wahren und Missbrauch zu verhindern.

Schutz vor Identitätsdiebstahl: Wenn persönliche Informationen in die falschen Hände geraten, können sie missbräuchlich verwendet werden, um die Identität der betroffenen Person zu stehlen.

Beispiel: Mit dem Personalausweis und anderen persönlichen Informationen kann jemand auf betrügerische Weise Kredite oder Verträge im Namen der betroffenen Person abschließen.

Schutz der Privatsphäre: Jeder Mensch hat das Recht, zu entscheiden, welche Informationen über ihn für andere sichtbar sind.

Beispiel: Auf sozialen Netzwerken können Bilder und persönliche Informationen von anderen missbraucht werden, wenn diese ohne Zustimmung geteilt werden.

1.2.3 Warum Firmendaten auf Computern und mobilen Geräten geschützt werden müssen

Firmendaten enthalten oft vertrauliche Informationen über das Unternehmen selbst, seine Mitarbeiter oder Kunden. Der Schutz dieser Daten ist wichtig, um Geschäftsprozesse sicher und professionell zu halten.

- **Vermeidung von Diebstahl und Sabotage:** Daten wie Geschäftsgeheimnisse und Finanzinformationen dürfen nicht in die Hände unbefugter Personen gelangen.

Beispiel: Ein Angriff auf die IT-Sicherheit eines Unternehmens könnte zur Veröffentlichung von Geschäftszahlen führen, was das Unternehmen wirtschaftlich stark schädigen könnte.

- **Schutz vor betrügerischer Verwendung:** Wenn Unbefugte Zugriff auf Firmendaten erhalten, könnten diese Daten genutzt werden, um dem Unternehmen finanziellen oder rechtlichen Schaden zuzufügen.

Beispiel: Kriminelle könnten Kundendaten eines Unternehmens verwenden, um Kreditkarteninformationen zu stehlen.

- **Vermeidung von unabsichtlichem Datenverlust:** Auch unabsichtliche Fehler können zu Datenverlust führen. Sicherheitsvorkehrungen sorgen dafür, dass solche Fehler minimiert und wichtige Daten gesichert werden.

Beispiel: Der Verlust eines ungesicherten Laptops mit sensiblen Kundendaten kann das Vertrauen der Kunden nachhaltig beeinträchtigen.

1.2.4 Allgemeine Grundsätze für Datenschutz und Privatsphäre: Transparenz, Notwendigkeit, Verhältnismäßigkeit

Datenschutz ist nicht nur wichtig, um Daten zu sichern, sondern auch, um Vertrauen zu schaffen. Es gibt zentrale Datenschutzprinzipien, die sicherstellen, dass Daten verantwortungsvoll verarbeitet werden.

- **Transparenz:** Personen müssen informiert sein, warum und wie ihre Daten genutzt werden.

Beispiel: Ein Online-Shop sollte seine Kunden darüber informieren, dass ihre Adressdaten für den Versand gespeichert werden und wie lange diese Daten aufbewahrt werden.

- **Notwendigkeit:** Es dürfen nur die Daten erhoben und gespeichert werden, die wirklich gebraucht werden.

Beispiel: Ein Fitnessstudio benötigt die Kontaktdaten seiner Mitglieder, jedoch nicht ihre detaillierten Krankengeschichten.

- **Verhältnismäßigkeit:** Die erhobenen Daten und deren Verarbeitung müssen in einem angemessenen Verhältnis zum Zweck stehen.

Beispiel: Ein Unternehmen, das lediglich ein Gewinnspiel veranstaltet, sollte nur die Daten abfragen, die zur Durchführung nötig sind, wie Name und E-Mail-Adresse.

1.2.5 Betroffene Personen und Inhaber der Datensammlung

Betroffene Personen und Inhaber der Datensammlung sind zwei wichtige Begriffe im Datenschutz.

- **Betroffene Personen:** Dies sind die Personen, deren Daten gesammelt werden. Sie haben das Recht zu erfahren, wie ihre Daten verwendet werden, und können gegebenenfalls verlangen, dass ihre Daten gelöscht oder berichtigt werden.

Beispiel: Ein Kunde, dessen E-Mail-Adresse in einem Online-Shop gespeichert wird, ist die betroffene Person und kann entscheiden, ob seine Daten gelöscht werden sollen.

- **Inhaber der Datensammlung:** Dies sind Organisationen oder Unternehmen, die Daten speichern und für deren Schutz verantwortlich sind. Sie müssen sicherstellen, dass die Daten sicher und nur zu den zulässigen Zwecken genutzt werden.

Beispiel: Ein Unternehmen, das die Kundendaten für Marketingzwecke speichert, ist der Inhaber der Datensammlung und muss diese Daten vor unbefugtem Zugriff schützen.

1.2.6 Einhaltung von Grundsätzen und Richtlinien bei der Nutzung von IKT

In der Informationstechnologie ist es wichtig, dass alle Mitarbeiter die Richtlinien des Unternehmens zur Datensicherheit einhalten.

Warum ist die Einhaltung von Richtlinien wichtig?

- Richtlinien helfen, den sicheren Umgang mit Daten sicherzustellen und unabsichtliche Fehler zu vermeiden. Sie geben klare Anweisungen, wie Daten verwendet, gespeichert und geschützt werden sollen.

Wie werden Richtlinien bekannt gemacht?

- Unternehmen informieren ihre Mitarbeiter über Richtlinien durch Kurse, Handbücher und Online-Richtlinienportale. So können alle sicherstellen, dass sie sich an die Vorschriften zur Datensicherheit halten.