IT – Security | Grundbegriffe zu Sicherheit

1. Datenbedrohung

1.1.1 Zwischen Daten und Informationen unterscheiden können

Daten sind rohe, unverarbeitete Werte oder Fakten, die keinen Kontext oder Zusammenhang haben**. Beispiele:** *Zahlen, Wörter, Messwerte*.

	A	B	C	D	E
1	College Enrollment 2016 - 2017				
2	Student ID	Last Name	Initial	Age	Program
3	ST348-245	White	R.	21	Drafting
4	ST348-246	Wilson	P.	19	Science
5	ST348-247	Thompson	A.	18	Arts
6	ST348-248	Holt	R.	23	Science
7	ST348-249	Armstrong	J.	37	Drafting
8	ST348-250	Graham	S.	20	Arts
9	ST348-251	McFadden	H.	26	Business
10	ST348-252	Jones	S.	22	Nursing
11	ST348-253	Russell	W.	20	Nursing
12	ST348-254	Smith	L.	19	Business
13					
14					
15					
16					

Informationen entstehen, wenn Daten in einen Zusammenhang gebracht werden und Bedeutung haben. **Beispiel:** *Eine Liste von Zahlen wird zur Information, wenn man weiß, dass es sich um eine Liste von Schulnoten handelt*.

Detailliertes Beispiel:

Stellen wir uns vor, dass eine Schule Daten zur Anwesenheit und Leistung der Schülerin Mathematik sammelt.

Rohdaten (Daten):

In einer Tabelle stehen Zahlen wie: 75, 80, 92, 68, und Wörter wie „fehlend“, „anwesend“. Für sich allein betrachtet sagen diese Daten wenig aus. Die Zahl „75“ könnte z. B. eine Prozentzahl, eine Punktzahl oder eine andere Form von Bewertung sein.

Interpretierte Daten (Informationen):

Wenn man weiß, dass „75“ die Prozentpunkte für eine Mathematikprüfung sind, wird aus dem Wert „75“ die Information, dass ein Schüler 75 % der möglichen Punkte erreicht hat. Daten wie „anwesend“ oder „fehlend“ werden zur Information, wenn sie in Zusammenhang mit den Anwesenheitslisten der Schüler und dem Datum eines bestimmten Schultages gebracht werden.

1.1.2 Die Begriffe Cybercrime und Hacken verstehen

Cybercrime (Cyberkriminalität) bezeichnet alle kriminellen Aktivitäten, die mit Hilfe von Computern, Netzwerken oder dem Internet durchgeführt werden. Dazu zählen Datendiebstahl, Online-Betrug, Phishing (Betrugsmethoden per E-Mail), Identitätsdiebstahl und der Missbrauch von Kreditkartendaten.

Hacken ist der Vorgang, unautorisiert auf Computersysteme oder Netzwerke zuzugreifen. Hacken kann unterschiedliche Ziele haben:

- Böswilliges Hacken und Cracking: Ziel ist Schaden oder Datendiebstahl.
- Ethical Hacking: Sicherheitsprüfungen durch "ethische" Hacker, die Systeme testen, um Schwachstellen zu finden, zu melden und zu beheben.

1.1.3 Böswillige und unabsichtliche Bedrohung für Daten durch Einzelpersonen, Dienstleister und externe Organisationen kennen

Böswillige Bedrohungen:

- **Einzelpersonen:** Ein Angestellter, der Daten absichtlich stiehlt oder manipuliert.
- **Dienstleister:** Externe Unternehmen könnten Daten zu illegalen Zwecken nutzen, z. B. für Werbezwecke ohne Zustimmung.
- **Externe Organisationen:** Hacker oder Cyberkriminelle, die Datenbanken angreifen, um vertrauliche Informationen zu stehlen.

Unabsichtliche Bedrohungen:

- **Einzelpersonen:** Ein Mitarbeiter löscht versehentlich wichtige Daten.
- **Dienstleister:** Ein IT-Service könnte ein Update einspielen, welches zu Datenverlust führt.
- **Externe Organisationen:** Externe Firmen, die für Datenverarbeitung zuständig sind, könnten versehentlich Daten veröffentlichen oder verlieren.

1.1.4 Bedrohung für Daten durch höhere Gewalt kennen

Daten können auch durch Ereignisse bedroht werden, auf die man keinen Einfluss hat (Höhere Gewalt), z. B.:

- Feuer: Zerstörung der Hardware und damit auch der gespeicherten Daten.
- Hochwasser: Flüssigkeitsschäden an Servern und Computern, die Daten speichern.
- Krieg: Angriffe oder Sabotage an Rechenzentren, um den Zugang zu wichtigen Daten zu verhindern.
- Erdbeben: Strukturschäden an Rechenzentren oder Gebäuden, was den Verlust der dort gespeicherten Daten verursachen kann.

Maßnahmen: Backups (Sicherung von Daten) an einem sicheren Standort speichern und Sicherungskopien regelmäßig aktualisieren.

1.1.5 Bedrohung für Daten durch die Verwendung von Cloud-Computing kennen

Cloud-Computing bietet viele Vorteile, birgt jedoch auch Risiken:

- **Datenkontrolle:** Da Daten auf Servern von Drittanbietern gespeichert werden, gibt man ein Stück weit die Kontrolle darüber ab. Es besteht das Risiko, dass der Anbieter die Daten verwendet oder sie mit anderen teilt.
- **Möglicher Verlust der Privatsphäre:** Daten in der Cloud können anfälliger für unberechtigte Zugriffe sein. Anbieter könnten gehackt werden, was sensible Daten in Gefahr bringt.

Maßnahmen zur Sicherheit:

- Starke Passwörter und Zwei-Faktor oder Multi-Faktor-Authentifizierung verwenden.
- Anbieter sorgfältig auswählen und prüfen, ob dieser ausreichende Sicherheitsvorkehrungen hat.
- Verschlüsselung einsetzen, um sicherzustellen, dass sensible Daten auch bei einem Datenleck geschützt bleiben.

Nicht vergessen!

IT-Sicherheit ist wichtig, um Daten und Informationen vor Bedrohungen zu schützen. Ob durch Menschen, Naturkatastrophen oder Technologie – Bedrohungen können viele Formen annehmen. Ein gutes Verständnis und präventive Maßnahmen wie regelmäßige Datensicherungen und der sorgfältige Umgang mit Cloud-Diensten sind entscheidend für den Schutz sensibler Informationen.