Datenbedrohungen

In der digitalen Welt lauern verschiedenste **Gefahren** für unsere Daten. Von **böswilligen Angriffen** über **unbeabsichtigte Fehler** bis hin zu **Naturkatastrophen** und den Herausforderungen im Zusammenhang mit **Cloud-Computing** gibt es viele Ursachen, warum Daten verloren gehen können.

Stell dir vor, jemand versucht, in dein soziales Netzwerk einzudringen und deine Nachrichten zu lesen. Das wäre ein böswilliger Angriff auf deine Daten.

Böswillige Bedrohungen ...
treten auf, wenn Menschen absichtlich versuchen, in Computersysteme einzudringen, um Daten zu stehlen, zu ändern oder zu zerstören.
Um sich vor böswilligen Bedrohungen zu schützen, sollten starke Passwörter verwendet, Sicherheitssoftware installiert und verdächtige E-Mails vermieden werden.

1) **Malware:** Böswillige Software, wie Viren oder Trojaner, kann auf einem Computer installiert werden, um schädliche Aktivitäten durchzuführen.
2) **Phishing-Angriffe:** Betrügerische E-Mails oder gefälschte Websites werden verwendet, um Benutzer dazu zu verleiten, vertrauliche Informationen preiszugeben.
3) **Hacker-Angriffe:** Personen mit bösen Absichten können versuchen, in Computersysteme einzudringen, um unbefugten Zugriff auf sensible Daten zu erhalten.

Stell dir vor, du hast wichtige Dateien auf deinem Laptop, und dann passiert ein Stromausfall, der deinen Laptop beschädigt. Das wäre wie eine unabsichtliche Bedrohung für deine Daten.

Unbeabsichtigte Bedrohungen ...
treten auf, wenn Menschen versehentlich Fehler machen oder unachtsam mit Daten umgehen, was zu Datenverlust oder -beschädigung führen kann.
Um sich vor unbeabsichtigten Bedrohungen zu schützen, sollten regelmäßige Backups erstellt, Schulungen zum Datenschutz durchgeführt und sicherheitsbewusstes Verhalten gefördert werden.

1) **Menschliche Fehler:** Das Löschen wichtiger Dateien oder das Überschreiben von Daten durch Fehler können zu unbeabsichtigten Bedrohungen führen.
2) **Datenausfälle:** Hardwarefehler oder Stromausfälle können zu Datenverlust führen, wenn keine angemessenen Sicherheitsvorkehrungen getroffen wurden.
3) **Fehlendes Sicherheitsbewusstsein:** Wenn Mitarbeiter nicht ausreichend über Sicherheitsmaßnahmen informiert sind, können sie versehentlich Sicherheitslücken schaffen.

Sowohl bewusste als auch unbeabsichtigte Handlungen können zu erheblichen Konsequenzen für die Sicherheit von Daten führen und müssen **deshalb gleichermaßen ernst genommen** werden!

Stell dir vor, du speicherst wichtige Fotos auf deinem Handy. Plötzlich kommt es zu einem schweren Hochwasser, das dein Zuhause erreicht und dein Handy beschädigt. In so einem Fall spricht man von höherer Gewalt.

① Welche Arten von höherer Gewalt kennst du? Zähle auf.

Höhere Gewalt:
Manchmal gibt es Naturkatastrophen oder große Unfälle wie Feuer oder Hochwasser. Solche Ereignisse könnten auch unsere Computer und die darauf gespeicherten Daten beeinträchtigen.
Um unsere Daten vor solchen Ereignissen zu schützen, sollten wir Backups anfertigen und diese an verschiedenen Orten aufbewahren, z. B. in der Cloud oder auf externen Festplatten.

Stell dir vor, du speicherst deine Fotos online in einem Cloud-Service, aber dann erfährst du, dass jemand unbefugten Zugriff darauf hatte. Das wäre wie eine Bedrohung für deine Daten in der Cloud.

Bedrohungen für Daten durch Cloud-Computing:
Cloud-Computing ist wie ein virtueller Speicherplatz im Internet, wo wir unsere Dateien speichern können. Aber manchmal müssen wir darauf achten, dass unsere Daten sicher sind, wenn sie in dieser „Wolke" liegen.
Um sicherzustellen, dass unsere Daten in der Cloud geschützt sind, sollten wir sichere Passwörter verwenden, die Zwei-Faktor-Authentifizierung aktivieren und die Sicherheitseinstellungen des Cloud-Dienstes überprüfen.

② Schau dir das Video So funktioniert die Zwei-Faktor-Authentisierung an.
Fülle dabei passende Wörter in die Lücken ein.

Ein _____ allein bietet nach aktuellen Sicherheitsstandards nicht mehr den bestmöglichen _____. Deswegen gibt es die 2-Faktor-Authentisierung oder die Anmeldung in _____. Wie es der Name schon andeutet, ist bei dieser _____ eine Abfolge aus zwei Faktoren zentral. Setzt ein Faktor _____ voraus, sollte der andere auf Biometrie oder auf _____ basieren. Das könnte z. B. dann so aussehen: Im ersten Schritt gibst du dein Passwort ein, im zweiten Schritt dann ein Einmal _____. Weitere mögliche Varianten sind das Einlesen einer _____, die Eingabe einer _____ oder ein _____scan mit einem Handy.

③ Entscheide, um welche Art der Datenbedrohung es sich handelt.

		bös-willig	unbeab-sichtigt	höhere Gewalt
1)	Ein Virus wird absichtlich auf einen Computer übertragen, um Daten zu beschädigen oder zu stehlen.	○	○	○
2)	Ein Mitarbeiter teilt versehentlich einen Ordner in der Cloud mit sensiblen Geschäftsdaten öffentlich, anstatt sie intern zu teilen.	○	○	○
3)	Eine gefälschte E-Mail, die vorgibt, von einer vertrauenswürdigen Quelle zu stammen, verleitet den Benutzer dazu, sensible Informationen preiszugeben.	○	○	○
4)	Ein Stromausfall führt zu einem Hardwarefehler, der zu einem Datenverlust führt.	○	○	○
5)	Ein starker Regen führt zu einer Überschwemmung im Serverraum, was zu physischen Schäden an den Servern und Datenverlust führt.	○	○	○
6)	Ein Mitarbeiter löscht versehentlich wichtige Dateien, die nicht wiederhergestellt werden können.	○	○	○
7)	Ein Brand in einem Rechenzentrum zerstört Server und führt zu einem massiven Datenverlust.	○	○	○
8)	Ein Hacker erhält unbefugten Zugriff auf die Cloud-Speicher eines Benutzers und stiehlt persönliche Fotos.	○	○	○
9)	Ein Mitarbeiter gibt unbeabsichtigt einem Kollegen Zugriff auf sensible Daten, die er nicht sehen sollte.	○	○	○