**Eine Auswahl verschiedener Sicherheitsziele:**

1. Die **Vertraulichkeit**: Schutz vor unberechtigtem Einblick

Die Daten müssen davor geschützt werden, dass unberechtigte Personen sie einsehen können. Eng an die Vertraulichkeit geknüpft ist auch die Privatsphäre: Schutz der persönlichen Daten.

1. Die **Integrität**: Sicherstellung der Unveränderlichkeit der Originaldaten

Die Daten sind nicht von dritten Personen oder einem Informatiksystem verändert worden, sondern sie sind in der Originalform.

1. Die **Verfügbarkeit** / die **Zuverlässigkeit**: Schutz vor dem Systemausfall

Stellt ein Informatiksystem einen wichtigen Dienst bereit, ist es sehr wichtig, dass sie zuverlässig funktionieren.

1. Die **Authentifikation** / die **Authentizität**: Feststellung der Identität

Für viele Dienste muss festgestellt werden, ob eine Person tatsächlich die ist, für die sie sich ausgibt. Die Authentifikation wird oft verwendet, wenn eine Zugriffskontrolle existiert.   
Die Authentizität ist die Sicherstellung, dass bestimmte Daten von einer Person gesendet wurden.

1. Die **Zugriffskontrolle**: Zugriff nur durch berechtigte Personen

Der Zugriff auf bestimmte Daten oder Dienste wird nur ausgewählten Personen erlaubt. Eine Zugriffskontrolle ist häufig mit einer Authentifikation verbunden.

1. Die **Anonymität** / die **Pseudonymität**: Geheimhaltung der Identität einer Person

In vielen Situationen ist es wichtig, dass bestimmte Daten nicht einer Person zugeordnet werden können, um Persönlichkeitsrechte nicht zu verletzten oder sich bestimmten Gefahren nicht auszusetzen. Eine weichere Form von Anonymität ist die Pseudonymität: Die Zuordnung zwischen Pseudonym und Identität wird geheim gehalten.

1. Die **Unbeobachtbarkeit**: Verdeckung einer Kommunikation

In bestimmten Situationen ist es wichtig, dass eine Kommunikation nicht für andere zu erkennen ist. Wenn man jemand weiß, dass zwei Personen kommuniziert haben, kann er manchmal darauf schließen kann, was der Inhalt der Kommunikation war.

1. Die **Verbindlichkeit**:

Getroffene Zusagen von Personen müssen eingefordert werden können.

Die Sicherheitsziele Vertraulichkeit (engl. **C**onfidentiality), Integrität (engl. **I**ntegrity) und Verfügbarkeit (engl. **A**vailability) sind die drei klassischen, vorrangigen Sicherheitsziele: Die sogenannte „CIA-Triad“.

**Beispiele, in denen Sicherheitsziele eine Rolle spielen**

1. Abiturklausuren (Vertraulichkeit, Zugriffskontrolle)

In der Nacht vor den zentralen schriftlichen Prüfungen im Fach Informatik wird ins Sekretariat der Schule eingebrochen. Am nächsten Morgen wird festgestellt, dass der Safe nicht geöffnet wurde und nichts gestohlen wurde. Allerdings findet man ein Notebook, dass per USB an den Kopierer angeschlossen ist, auf dem die Abiturklausuren kopiert wurden.

1. Geheime Zettelbotschaften (Vertraulichkeit, Authentizität)

Während einer Unterrichtsstunde erhält Kerim unauffällig einen im Kurs herumgereichten Zettel, auf dem seine Mitschülerin Annika ihm einen Ort für ein Treffen nach dem Unterricht vorschlägt. Sein Sitznachbar, der anscheinend den Zettel gelesen hat, beginnt ihn damit zu ärgern. Seltsam findet er auch, dass er mit Annika schon einen Treffpunkt vereinbart hatte. Davon ist in dem Zettel aber nichts zu lesen. Auch die Schrift sieht irgendwie etwas seltsam aus.

1. Wahlen (Vertraulichkeit, Integrität, Zuverlässigkeit)

An einer Schule wird von einem Differenzierungskurs Informatik eine App entwickelt, mit der die Klassen ihre Klassensprecherinnen und Klassensprecher online wählen können. Jede Schülerin und jeder Schüler erhalten einen Account auf dem „Wahlserver“. Bei dem Account wird der Benutzername, das Passwort und die Klassenzugehörigkeit verwaltet. Die Schülerinnen und Schüler können nun zunächst bis zu einem Stichtag Vorschläge für die Klassensprecherin bzw. den Klassensprecher machen. Nach dem Stichtag haben die Schülerinnen und Schüler 3 Tage Zeit, ihre Stimme abzugeben. Nach der Wahl gibt es jedoch Ärger in der Klasse. Während Sergej sich beschwert, dass der Server nicht zu erreichen war, als er abstimmen wollte, wundert sich Vanessa, dass sie nur 3 Stimmen bekommen hat, obwohl ihre sieben Freundinnen sie alle wählen wollten. Kira hat gar nicht abgestimmt, da sie Angst hatte, jemand aus dem Differenzierungskurs könnte nachsehen, wie sie abgestimmt hat.

1. Klausurnote (Integrität, Vertraulichkeit)

Karl bringt seiner Zwillingsschwester Karla, die erkrankt ist, ihre Deutschklausur aus der Schule mit. Mit einem gehässigen Lächeln überreicht er ihr die Klausur. Karla ist unfassbar enttäuscht, weil die Note mangelhaft unter der Klausur steht, obwohl sie ein sehr gutes Gefühl bei der Klausur hatte. Bisher hatte sie immer mindestens die Note gut. Auch die schriftliche Rückmeldung ihrer Lehrerin klingt überhaupt nicht nach einer schlechten Note. Sie sieht sich die Note, die ihre Lehrerin unter die Klausur geschrieben hat, genau an und stellt fest, dass oberhalb der Note anscheinend gekillert wurde. Sie probiert, den Rotstift der Lehrerin zu killern und ist erfolgreich.

1. Kopierer (Zugriffskontrolle)

In einem Schulzentrum steht an zentraler Stelle ein Kopierer, der mit einer Kopierkarte und einer PIN genutzt werden kann. In den Sekretariaten der Schule kann eine Kopierkarte erworben werden. Die Kopierkarte ist mit einem Guthaben aufgeladen, so dass man eine bestimmte Zahl von Kopien auf dem Kopierer machen kann.

1. Whistle-Blowing (Anonymität, Unbeobachtbarkeit)

In einer öffentlichen Schule in Absurdistan erhält ein Lehrer per Mail von seiner Schulleiterin eine Anweisung, die seiner Meinung nach rechtswidrig ist. Er merkt dies gegenüber seiner Schulleiterin im Gespräch an, wird von dieser jedoch zurechtgewiesen. Als er die Anweisung nicht umsetzt, wird er von ihr unter Druck gesetzt. Er möchte die per Mail gesendete Anweisung an eine vertrauenswürdige Journalistin weitergeben, traut sich jedoch nicht, da er die Konsequenzen fürchtet. Außerdem möchte er nicht, dass die Journalistin die Mail zu ihm zurückverfolgt.

1. Keyless-Entry für Fach-Räume (Zugriffskontrolle, Authentifikation)

In einer neu ausgestatteten Schule wird ein „Keyless-Entry“-System für die Fach-Räume eingesetzt. Jede Lehrerin und jeder Lehrer besitzt einen Funkchip am Schlüsselbund. Die Tür des Fachraums besitzt keine Klinke und kann in der Regel nicht aufgedrückt werden. Wenn sich ein Funkchip im Raum befindet oder auf dem Gang vor der Tür ist, kann die Tür aufgedrückt werden.   
Nach einer kurzen Einsatzzeit wird festgestellt, dass Schülerinnen und Schüler bereits in den Fachräumen sitzen, bevor deren Lehrerin bzw. Lehrer anwesend sind. Die Türen der Fachräume entriegeln sich auch, wenn eine andere Lehrerin bzw. ein anderer Lehrer mit dem Funkchip in der Tasche an der Tür vorbeigeht.

1. Bestellung in der Schulmensa (Verbindlichkeit, Authentizität)

Schülerinnen und Schülern können das Mittagessen in der Schulmensa vorbestellen. Dazu öffnen sie im Browser die Seite der Mensa und wählen aus den angegebenen Gerichten eins aus.   
Der Mensabetreiber hat das Problem, dass für heute mehr als doppelt so viele Mittagessen bestellt wurden, wie Schülerinnen und Schüler an der Schule sind.

1. Mogeln in der Klausur (Vertraulichkeit, Unbeobachtbarkeit)

Fabienne fragt in einer Klausur Onur nach einem leeren Klausurbogen. Onur hält ihn hoch, um dem Aufsicht führenden Lehrer zu zeigen, dass das Blatt leer ist. Der Lehrer nimmt den Klausurbogen und öffnet ihn. Er stellt fest, dass auf der Innenseite viele mit Bleistift geschriebene Notizen zur Klausur sind.