1 Sicherheitsziele

Absolute Sicherheit ist nicht erreichbar. Selbst nach raffiniertesten Verfahren erstellte kryptografische Schlüssel können im Prinzip –mit viel, viel Glück– beim ersten Versuch erraten werden.

Sicherheitsziele werden häufig nur unter drei Schlagwörtern abgehandelt:

- Verfügbarkeit (*availability*),
- Integrität (*integrity*),
- Vertraulichkeit (*confidentiality*),

Der Begriff der Sicherheit wird dann auf der Ebene dieser Ziele definiert:

- Ein Rechensystem wird als **sicher** angesehen, wenn es die Sicherheitsziele seiner Teilnehmer bzgl. Verfügbarkeit, Integrität und Vertraulichkeit erfüllt.

Wir betrachten im folgenden diese Sicherheitsziele etwas genauer am Beispiel einer **Nachrichten-übertragung**, bei der ein Sender `S` eine Nachricht `m` an einen Empfänger `R` überträgt.

Grob kann man folgende Einteilung treffen:

Bedrohung	Schutz der Kommunikations-	
	Inhalte	Umstände
Unautorisierte Beeinträchtigung der Nutzbarkeit (Verfügbarkeitsziele)	Verfügbarkeit	Erreichbarkeit Verbindlichkeit
Unautorisierte Änderung von Information (Integritätsziele)	Integrität	Zurechenbarkeit Pseudonymität
Unautorisierter Zugriff auf Information (Vertraulichkeitsziele)	Vertraulichkeit	Anonymität Unbeobachtbarkeit

Das gleiche Sicherheitsziel kann aus ganz unterschiedlichen Interessenslagen entstehen, wie folgende Beispiele zeigen:

Ziele	aktiv	passiv
Erreichbarkeit	A möchte (für B) erreichbar sein	B möchte A stets erreichen können
Verbindlichkeit	A möchte die Zusagen (von B) rechtlich durchsetzen können	B möchte die Zusagen (von A) rechtlich durchsetzen können

1.1 Verfügbarkeit von Diensten

1.1.1 Nutzbarkeit

Wenn für die betrachtete Anwendung der Dienst der Nachrichtenübertragung nützlich ist, so gibt es Teilnehmer, die ein Interesse an seiner **Verfügbarkeit** (*availability*) haben.

Diese Teilnehmer erwarten, dass eine von ihnen gewünschte Nachrichtenübertragung mit den von ihnen angebenen Parametern zu der von ihnen gewünschten Zeit ausgeführt wird.

Das Ziel der Verfügbarkeit kann auch stufenweise reduziert werden.
Vorrangig wird die tatsächliche Ausführung erwartet.
Nachrangig wird für den Fall der Nichterfüllung des Dienstes gefordert, dass eine geeignete **Fehlerbehandlung** (*exception handling*) durchgeführt wird.

Diese kann beispielsweise aus

- einer sinnvollen Teilausführung des Dienstes,
- einer geeigneten Ersatzhandlung oder
- einer Benachrichtigung über den Fehlerfall

bestehen.

Man kann dann das Gesamtinteresse auch so ausdrücken, dass der um die Fehlerbehandlung erweiterte Dienst immer verfügbar ist.

1.1.2 Erreichbarkeit

Dieses Ziel beschreibt, dass man jederzeit –wenn gewünscht– einen Nutzer oder eines Maschine **erreichen** kann, also zu ihm/ihr Kontakt aufnehmen kann.

1.1.3 Verbindlichkeit

Dieses Ziel beschreibt, dass ein Nutzer belangt werden kann, um seine Zusagen innerhalb einer angemessenen Zeit zu erfüllen, seine Zusagen also **verbindlich** sind.

1.2 Integrität von Daten

1.2.1 Zutreffen der Nachricht

In vielen Anwendungen hat die vom Sender an den Empfänger übermittelte Nachricht `m` eine inhaltliche Bedeutung in der realen Welt.

So beziehen sich z.B. Nachrichten, die zu oder von einer **Datenbank** übertragen werden, auf den in der Datenbank dargestellten Ausschnitt der Welt.

Beispiel: Soll die Datenbank z.B. den Lagerbestand eines Unternehmens darstellen, so verlangt man, dass die Datenbank ein **zutreffendes** Abbild des wirklichen Lagers ist.

Jede durch eine Nachricht an die Datenbank ausgelöste Änderung des Datenbankzustandes soll die Übereinstimmung der Datenbank mit (dem modellierten Ausschnitt) der realen Welt bewahren;
jede von der Datenbank als Antwort einer Anfrage übertragene Nachricht soll ebenfalls mit (diesem Ausschnitt) der realen Welt übereinstimmen.

Da sich der gewünschte Zusammenhang zwischen Datenbank und realer Welt grundsätzlich nicht formal ausdrücken und algorithmisch behandeln lässt,
überwacht man ersatzweise Bedingungen –**semantische Bedingungen** oder **Integritätsbedingungen** (*integrity constraints*)–, die (nur) an den Zustand (und nicht an die Zustandsübergänge) der Datenbank gestellt werden.

Der ursprüngliche Dienst der Nachrichtenübertragung wird dadurch erweitert um den zusätzlichen –stets automatisch auszuführenden– Dienst der Überwachung der Einhaltung der Integritätsbedingungen (**Integritätsüberwachung**).

Beispiel: In einem rechnergestützten **Zahlungssystem** beziehen sich Nachrichten auf Geldwerte.

Hier sollen den Nachrichtenübertragungen im Rechensystem Zahlungsvorgänge in der Welt entsprechen.

Der gewünschte Zusammenhang zwischen dem Zahlungssystem und der wirklichen Welt entzieht sich auch hier der unmittelbaren formalen Behandlung, so dass man ersatzweise wieder Integritätsbedingungen an die Gesamtheit der Nachrichtenübertragungen und der dadurch ausgelösten Kontenbewegungen stellt.

Z.B. kann man fordern, dass die Summe der auf den Konten dargestellten Zahlen konstant bleibt.

1.2.2 unveränderter Zustand

Das inhaltliche Zutreffen von Nachrichten setzt i.a. voraus, dass eine Nachricht vom Empfänger in einem **unveränderten Zustand** empfangen wird, also so, wie sie vom Sender verschickt wurde.

Wird die Nachricht über eine weite Entfernung übertragen, so dürfen weder physische Einwirkungen auf die Übertragungswege noch andere Teilnehmer, die die Übertragung vermitteln, die Nachricht verändern.

Wird die Nachrichtenübertragung zeitlich verzögert ausgeführt, insbesondere also wenn die Nachricht oder ihre Teile zwischenzeitlich in einer Datenbank aufgehoben werden, so muss der jeweilige Zustand des Datenspeichers unverändert bleiben.

Man kann die Betrachtungen noch weiter ausdehnen. Zusätzlich müssen in allen Fällen auch der Zustand der benutzten Programme und der ausgeführten Prozesse unverändert bleiben, weil man sonst nicht die ordnungsgemäße Ausführung des Dienstes erwarten kann.
Insbesondere muss das benutzte Programm identisch mit dem beabsichtigten Programm sein (und nicht unabsichtlich oder böswillig seit der Inbetriebnahme verändert worden sein), und
der ausgeführte Prozess muss wirklich das beabsichtigte Programm ausführen (und nicht etwa versehentlich oder böswillig einen Wechsel zu einem anderem Programm vornehmen).

Das Ziel der **Integrität** (*integrity*) im Sinne von **unverändertem Zustand** kann also sehr weitgehend gedeutet werden: es umfasst dann nicht nur die Nachrichten, sondern den gesamten Vorgang des Dienstes mit all seinen Komponenten wie Daten, Programmen und Prozessen. Diese weitgehende Deutung wird auch dadurch gerechtfertigt, dass alle Komponenten auf den unteren Schichten eines Rechensystems einheitlich zurückführbar sind auf Zustände von physischen Speichern oder von physischen Übertragungswegen. Dabei verwischen sich die Unterschiede zwischen den verschiedenen Typen der Komponenten.

1.2.3 Erkennen von Veränderungen

Wenn das Interesse am unveränderten Zustand von Daten oder Programmen nicht voll erfüllt werden kann, so kann man sich mit einer schwächeren Form von **Integrität** zufrieden geben: man erwartet dann nur noch, dass man **erkennen** kann, ob eine Veränderung vorliegt.

Zusätzlich kann man dann fordern, dass eine erkannte Veränderung wieder **behoben** werden kann, der ursprüngliche Zustand also wiederhergestellt werden kann.

1.2.4 zeitliche Richtigkeit

Manche Interessen treten erst dann zutage, wenn die Teilnehmer eines Rechensystems einander viele Nachrichten über einen größeren Zeitraum hinweg übertragen, wobei die Übertragung jeweils mit Hilfe dritter Teilnehmer ausgeführt wird.

Dann kann ein Interesse an **Integrität** im Sinne von **zeitlicher Richtigkeit** auftreten.

Z.B. kann die Forderung bedeutsam sein, dass ein Empfänger die für ihn bestimmten Nachrichten eines einzelnen Senders in der richtigen Reihenfolge erhält, also in derjenigen Reihenfolge, in der die Nachrichten gesendet wurden.

Oder der Empfänger erwartet, dass Nachrichten ihn im wesentlichen verzögerungsfrei erreichen oder dass er zumindest feststellen kann, ob sie "frisch gesendet" wurden.

1.2.5 Authentizität des Senders

Die bislang behandelten Ziele der Verfügbarkeit und der Integrität beziehen sich auf einen Dienst als Ganzes, hier insbesondere den Dienst der Nachrichtenübertragung, oder auf einen bedeutsamen Zustand des Dienstes, hier insbesondere Daten und Programme.

Weitere Interessen beziehen sich auf die **Teilnehmer** eines Dienstes. **Authentizität** bezeichnet das Interesse an der Richtigkeit des Senders eines Nachricht.

Dieses Interesse hat üblicherweise der Empfänger der Nachricht.

Dieser möchte sicher sein, dass eine empfangene Nachricht, die häufig auch Angaben über den Sender enthält, wirklich von dem Teilnehmer stammt, der als Sender angegeben ist.

1.2.6 Zuordbarkeit von Handlungen zu Benutzern

Der Betreiber eines Rechensystems muss den ordnungsgemäßen Betrieb des Rechensystems sicherstellen. Dabei muss er insbesondere die für dieses Rechensystem als berechtigt anerkannten Ziele unterstützen. Wie in jedem Lebensbereich muss man auch beim Betrieb eines Rechensystems darauf vorbereitet sein, dass Störungen des Betriebes und Verletzungen der Ziele auftreten können.

In diesem Zusammenhang besteht ein Interesse, dass man formale Handlungen im Rechensystem –insbesondere das Anstoßen von Nachrichtenübertragungen oder anderer Dienste– den einzelnen menschlichen Benutzern des Rechensystems genau **zuordnen** kann.

Dadurch legt man eine Grundlage dafür, dass man unerwünschte Handlungen im Rechensystem –unabsichtliche Ungeschicklichkeiten wie bösartige Angriffe– auf das Fehlverhalten von benennbaren Menschen zurückführen kann.

Diese Menschen kann man dann im Rahmen der dafür vorgesehenen Regeln für ihr Fehlverhalten verantwortlich machen.

1.2.7 Anerkennung von Verpflichtungen, Zurechenbarkeit, Bescheinigungen

Der Empfänger kann ein über die Authentizität hinausgehendes Interesse haben: er möchte sich dann nicht nur selbst vergewissern können, dass der angegebene Sender der tatsächliche ist, sondern zusätzlich in der Lage sein, dritten Teilnehmern zu **beweisen**, dass die empfangene Nachricht vom Sender stammt.

Dadurch soll gewährleistet werden, dass der Sender **anerkennen** muss, dass er die vorliegende Nachricht (mit der er vielleicht Verpflichtungen eingegangen ist) gesendet hat.

Der Sender kann dann die Nachricht (und damit seine Verpflichtungen) nicht abstreiten; sie ist ihm **zuzurechnen** (*accountability*).

Natürlich hat der Sender ein dazu spiegelbildliches Interesse: er möchte nur solche Nachrichten anerkennen müssen, die er tatsächlich gesendet hat.

Der Empfänger soll ihm keine nur vorgeblich von ihm stammende Nachricht anlasten können.

Die mit der Anerkennung von Nachrichten verbundenen Interessen entsprechen weitgehend den Erwartungen, die man üblicherweise mit Hilfe von handgeschriebenen **Unterschriften** erfüllt.

Wenn ein Sender eine Nachricht an einen Empfänger überträgt oder mit Hilfe anderer Teilnehmer übertragen lässt, dann können alle beteiligten Teilnehmer ein Interesse an **Bescheinigungen** bzgl. dieses Vorgangs haben.

Solche Bescheinigungen sollen dazu dienen, dass jeweils andere Teilnehmer die Ausführung von Teilvorgängen anerkennen müssen.

Z.B. kann der Sender sich von einem Teilnehmer, der die Übertragung ausführt, bescheinigen lassen, dass er eine Nachricht aufgegeben hat.

Oder der Sender, bzw. der die Übertragung ausführende Teilnehmer, lässt sich vom Empfänger bescheinigen, dass letzterer die Nachricht erhalten hat.

1.2.8 Pseudonymität

Pseudonyme ermöglichen einem Nutzer, eine Ressource oder einen Dienst zu benutzen, ohne seine Identität preiszugeben. Andererseits kann ihm diese Nutzung trotzdem zugerechnet werden.

1.3 Vertraulichkeit von Nachrichten

1.3.1 Vermeidung der Datenerhebung

Ein (zunächst trivial erscheinender, aber praktisch sehr bedeutsamer) Teilaspekt der Vertraulichkeit ist die **Vermeidung** der Erhebung und Speicherung unnötiger Daten.

Dazu muss vorab festgelegt werden, welche Daten wozu notwendig sind.

Auf das Senden einer entsprechenden Nachricht könnte dann verzichtet werden.

1.3.2 Geheimhaltung der Nachricht vor Fremden

Der Sender kennt üblicherweise die von ihm versandte Nachricht, und er wünscht sich häufig, dass seine Nachricht gezielt und ausschließlich an den von ihm bestimmten Empfänger übertragen wird.

Dieses Interesse an **Vertraulichkeit** (*confidentiality*) zielt auf die Richtigkeit des Empfängers.

Niemand anders als der gewünschte Empfänger soll die Nachricht erhalten, und niemand anders als der Sender oder der gewünschte Empfänger soll während der Übertragung die Nachricht lesen bzw. die Bedeutung der Nachricht folgern können.

Für verschiedene Teilnehmer und Betroffene eines Rechensystems kann das Interesse an Vertraulichkeit recht unterschiedlich ausfallen.

Z.B. werden für ein eingebettetes Rechensystem in einer hierarchischen Organisation Vertraulichkeitsanforderungen jeweils für einen Zweig der Organisation von oben angeordnet.

Dagegen sollen im Sinne der **informationellen Selbstbestimmung** diejenigen Personen, über die die Nachrichten etwas aussagen, auch über deren Verwendung selbstbestimmt entscheiden.

Im ersten Fall stehen die Bedürfnisse der Organisation im Vordergrund, im zweiten Fall wird ein in der Verfassung verankertes Grundrecht von freien Bürgern betont.
Die genannten und weitere Gesichtpunkte müssen i.a. auf der Grundlage von Wertentscheidungen und der Rangfolge von Rechtsgütern gegeneinander abgewogen werden.
Vorgaben hierzu geben einschlägige Gesetze, z.B. das **Bundesdatenschutzgesetz** und die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**Europäische Datenschutzrichtlinie**).

Für das Interesse an Vertraulichkeit ist wesentlich und unerlässlich, dass es allen Teilnehmern außer dem Sender und dem gewünschten Empfänger auch die Möglichkeit abspricht, die Bedeutung einer Nachricht zu folgern.
Die Durchsetzung dieses Interesses muss also nicht nur die eigentliche **Nachrichtenübertragung** beachten, sondern alle mit ihr verbundenen **Informationsflüsse** einschließlich derjenigen, die auf **Folgerungen** beruhen.

Ein Verlust der Vertraulichkeit ist i.a. ein dauerhafter Schaden; ein offengelegtes Geheimnis ist keines mehr.

Dies ist eine grundlegend andere Situation als bei einer Verletzung der Verfügbarkeit oder Integrität; die Verfügbarkeit oder Integrität kann i.a. durch geeignete Maßnahmen wiederhergestellt werden.

1.3.3 Unbeobachtbarkeit von Handlungen

Das Interesse an Vertraulichkeit der Nachricht kann noch verstärkt werden. Man kann nämlich fordern, dass die gesamte Handlung der Nachrichtenübertragung **unbeobachtbar** sein soll.

Die weitestgehende Forderung ist, dass kein Teilnehmer außer den unmittelbar mitwirkenden feststellen kann, dass überhaupt eine Nachrichtenübertragung stattfindet.

Etwas weniger weitgehend kann man erwarten, dass niemand außer dem Sender und dem Empfänger die Quelle und das Ziel der Nachrichtenübertragung bestimmen kann.

Natürlich darf so ein Interesse nicht derart übersteigert werden, dass die Anforderungen unerfüllbar werden und damit der Dienst der Nachrichtenübertragung überhaupt nicht mehr verfügbar ist.

1.3.4 Anonymität von Benutzern

Das Interesse der Anonymität gilt einer Sonderform von Unbeobachtbarkeit, nämlich der Identität, die z.B. im Zusammenhang mit rechnergestützten **Zahlungssystemen** bedeutsam ist.

Dabei fordert man, dass die unmittelbar an einer Nachrichtenübertragung (die beim Zahlungssystem einem Zahlungsvorgang entspricht) mitwirkenden Teilnehmer sich als sendender oder empfangener Teil wohlbestimmen können, ohne dabei ihre bürgerliche Identität preiszugeben.

Diese Teilnehmer können also die Nachrichtenübertragung **anonym** durchführen (und damit einen Zahlungsvorgang unter ähnlichen Bedingungen wie beim Überreichen von Münzen oder Geldscheinen abwickeln).

Das Interesse an Anonymität reicht über die reinen Zahlungssysteme weit hinaus und umfasst jegliche Art von **elektronischer Dienstleistung**. Ein bedeutsamer Sonderfall ist hier, dass die Inanspruchnahme einer elektronischen Dienstleistung –vorzugsweise elektronisch– bezahlt werden soll. Beispiele dafür sind rechnergestütze Auskunfts- und Buchungssysteme sowie elektronische Publikationssysteme einschließlich Systemen für vom Kunden abrufbare Videodienstleistungen. Wenn für solche Systeme ein Kunde (als Sender) durch eine Nachricht an den Dienstleister (als Empfänger) eine Dienstleistung anfordert und dann durch eine entgegengesetzte Nachricht diese Dienstleistung erhält, so können insbesondere die folgenden zwei Interessen auftreten:
Der Kunde möchte die Dienstleistung **anonym** erhalten und der Dienstleister möchte die Anforderung **anerkannt** wissen, um die Bezahlung der Dienstleistung sicherzustellen.

Das Interesse an Anonymität ist auch bedeutsam im Zusammenhang mit **(statistischen) Datenbanken**, die **zu wissenschaftlichen** oder **staatlichen Zwecken** betrieben werden.

Wenn man Bürger aus einem übergeordneten Interesse bittet oder gar gesetzlich verpflichtet, persönliche Daten, etwa über Krankheiten, an eine Datenbank zu übertragen, so kann man manchmal das Interesse der betroffenen Bürger an Vertraulichkeit und ihr Grundrecht auf informationelle Selbstbestimmung dadurch wahren, dass sie als Sender (oder als Betroffene) nur anonym auftreten.

1.3.5 Rollentrennung

Auch das Interesse der Rollentrennung (*separation of duties*) tritt in der Regel nur bei Rechensystemen auf, in denen viele verschiedenartige Nachrichten übertragen werden.

Zusätzlich stehen bei diesem Interesse die Sender und die Empfänger für in einem Unternehmen handelnde Menschen, insbesondere für mächtige Institutionen (z.B. Träger staatlicher Funktionen).

Die von den Nachrichten betroffenen Menschen –und dies sind häufig gerade nicht die Sender und die Empfänger der Nachrichten, sondern typischerweise Menschen, deren persönliche Daten in den Nachrichten weitergegeben werden– haben ein Interesse daran, dass Daten ausschließlich **zweckgebunden** genutzt werden.

Sie erwarten, dass ihr Recht auf **informationelle Selbstbestimmung** dadurch gewahrt wird, dass die im Unternehmen handelnden Menschen ihre unterschiedlichen **Handlungsrollen streng trennen**, indem sie Daten, über die sie in einer ersten Rolle befugt verfügen dürfen, nicht in einer zweiten Rolle missbräuchlich verwenden.

Manchmal ist es praktisch, dass eine Person für jede ihrer Rollen ein anderes **Pseudonym** benutzt.

1.3.6 Verdeckte Verpflichtungen

Die Liste von mit Nachrichtenübertragungen verbundenen Sonderinteressen erscheint unerschöpflich. Ein Beispiel hierfür sind sog. **verdeckte Verpflichtungen**.

Einerseits wird hierbei die vom Sender übertragene Nachricht als eine "Verpflichtung" gedeutet, die der Sender gegenüber dem Empfänger eingeht.

Andererseits kann der Empfänger zwar die Nachricht (als Zeichenkette) empfangen, aber die darin enthaltene Verpflichtung nicht selbst erkennen.

In diesem Beispiel hat der Sender insbesondere das Interesse, dass die in der Nachricht enthaltene Information über die Art seiner "Verpflichtung" selbst gegenüber dem Empfänger **vertraulich** bleibt.

Und der Empfänger hat insbesondere das Interesse, dass der Sender die Nachricht als solche **anerkennen** muss.

1.3.7 Abhören von Nachrichten

Obwohl Vertraulichkeit von Nachrichten zu den durch die Verfassung geschützten Rechtsgütern gehört, haben alle Regierungen ein Interesse und auch eingeschränkte Rechte, in Ausnahmefällen den Nachrichtenverkehr **abzuhören**, d.h. sowohl die Nachricht als solche zu bestimmen und ggf. aufzuzeichnen als auch ihre Bedeutung zu erkennen.