die Funktionssicherheit die Grundlage für die Informations- bzw. Datensicherheit eines Systems ist. Die Funktionssicherheit ist eng verwandt mit den Begriffen der Zuverlässigkeit bzw. der Verlässlichkeit.

Definition 1.3 (Verlässlichkeit)

Verlässlichkeit

Unter der Verlässlichkeit (engl. *dependability*) eines Systems verstehen wir die Eigenschaft, keine unzulässigen Zustände anzunehmen (Funktionssicherheit) und zu gewährleisten, dass die spezifizierte Funktion zuverlässig (engl. *reliability*) erbracht wird.

□

Safety

Zur Gewährleistung von Funktionssicherheit (Safety) setzt man Konzepte und Verfahren ein, die darauf abzielen, die Verlässlichkeit von IT-Systemen zu gewährleisten. Es handelt sich dabei im Wesentlichen um Maßnahmen zur Abwehr von solchen Bedrohungen, die durch das technische Fehlverhalten des IT-Systems selber (von innen) entstehen. Derartige Bedrohungen ergeben sich insbesondere durch Programmierfehler, die mit Techniken der Programmvalidierung oder -verifikation aufzudecken sind.

Im vorliegenden Buch beschäftigen wir uns mit der Sicherheit technischer Systeme im Sinne der englischen Begriffe *Security* und *Protection*. Behandelt werden Konzepte und Maßnahmen zur Abwehr von Bedrohungen, die durch unberechtigte Zugriffe auf die zu schützenden Güter des IT-Systems entstehen und im Wesentlichen von außen erfolgen. Anzumerken ist, dass die Grenzen zwischen Safety- und Security-Fragestellungen fließend sind und es durchaus Überlappungen gibt.

1.2 Schutzziele

Informationen bzw. Daten sind zu schützende Güter informationssicherer bzw. datensicherer Systeme. Der Zugriff auf diese ist zu beschränken und zu kontrollieren, so dass nur dazu autorisierten Subjekten ein Zugriff gewährt wird. Die Schutzziele, die diese Anforderungen präzisieren, sind die Datenintegrität und Informationsvertraulichkeit. Zugreifende Subjekte müssen eindeutig identifiziert und ihre Identität muss verifiziert sein. Die entsprechende Eigenschaft nennt man die Authentizität von Subjekten. Ist ein Subjekt authentifiziert und berechtigt, also autorisiert, einen Zugriff auf ein Objekt bzw. eine Information durchzuführen, dann sollte das System gewährleisten, dass dieser Zugriff auch möglich ist; man spricht von der Eigenschaft der Verfügbarkeit. Hat ein Subjekt einen Zugriff bzw. eine Aktion durchgeführt, so ist es vielfach notwendig, dass auch noch im Nachhinein die Urheberschaft des Zugriffs bzw. der Aktion eindeutig dem entsprechen-

den Subjekt zuordenbar ist. Man spricht hier von der Verbindlichkeit oder Zuordenbarkeit des Systems. Die angesprochenen Schutzziele werden nun im Folgenden präzisiert.

Definition 1.4 (Authentizität)

Authentizität

Unter der Authentizität eines Objekts bzw. Subjekts (engl. *authenticity*) verstehen wir die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist.

□

Authentifikation

Die Authentizität eines Subjekts bzw. Objekts wird durch Maßnahmen zur Authentifikation (engl. *authentication*) überprüft. Dazu muss nachgewiesen werden, dass eine behauptete Identität eines Objekts oder Subjekts mit dessen charakterisierenden Eigenschaften übereinstimmt.

Subjekt-Auth.

In herkömmlichen Systemen wird eine Authentifikation meist nur für Benutzer als Subjekte durchgeführt. Die Identifikation basiert auf der Vergabe von eindeutigen Benutzerkennungen (engl. *account*) oder Benutzernamen. Charakterisierende Eigenschaften zum Nachweis der Identität sind beispielsweise Passwörter, deren Kenntnis der Benutzer beim Systemzugang nachweisen muss, oder biometrische Merkmale wie Fingerabdrücke. Identitätsnachweise werden häufig allgemein als Credentials bezeichnet, womit man von dem spezifischen, zum Identitätsnachweis tatsächlich verwendeten Verfahren abstrahiert.

Objekt-Authentizität

Mit dem Übergang zu offenen Systemen werden auch zunehmend Maßnahmen erforderlich, die die Authentizität von Objekten, wie beispielsweise Web-Server, Access Points (bei 802.11 WLAN) oder Code nachweisen. Hierbei beschränkt man sich jedoch i.d.R. auf einfache Mechanismen, nämlich kryptografische Verfahren (vgl. Kapitel 7), um die Echtheit von Daten zu überprüfen, die über ein unsicheres Transportmedium wie dem Internet übertragen werden. Diese Echtheitsprüfung beschränkt sich auf einen Ursprungs- bzw. Urhebernachweis, ohne Aussagen über die Funktionalität des Objekts zu treffen. Die Authentizität eines Objekts im engeren Sinn würde den Nachweis erfordern, dass seine spezifizierte Funktionalität mit seiner tatsächlich erbrachten übereinstimmt. Entsprechende Nachweise, die z.B. unter Verwendung der Proof-Carrying-Code Technik [136] erstellt werden, sind sehr schwierig zu führen und werden in der Praxis noch nicht eingesetzt. Hier sind noch weitere, verstärkte Forschungsaktivitäten notwendig, da gerade mit der ansteigenden Mobilität von Daten und von mobilem Code und Apps (vgl. Kapitel 2.7) wie zum Beispiel der Java-Applets oder Apps für Android und Apple iPhone, ein Authentizitätsnachweis, der neben einem Ursprungsnach-

weis auch eine Aussage über eine korrekte Funktionalität beinhaltet, für die Sicherheit offener Systeme dringend erforderlich ist.

Definition 1.5 (Datenintegrität)

Integrität

Wir sagen, dass das System die Datenintegrität (engl. *integrity*) gewährleistet, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.

□

Rechtefestlegung

Die Eigenschaft der Datenintegrität erfordert zum einen die Festlegung von Rechten zur Nutzung von Daten. Beispiele hierfür sind Lese- oder Schreibberechtigungen für Dateien oder das Recht, von einem bestimmten Konto einen Betrag bis zu einer festgelegten Obergrenze abheben zu dürfen. Zum anderen sind Rechte an Subjekte zu vergeben, so dass diese autorisiert sind, die entsprechenden Zugriffsrechte wahrzunehmen. Abhängig von den damit getroffenen Festlegungen können Integritätsaussagen unterschiedlicher Qualität gemacht werden. So wird beispielsweise durch die Vergabe von Schreibberechtigungen an Dateien die Möglichkeit zur Modifikation des Datei-Objekts nicht weiter beschränkt, so dass Subjekte zu beliebigen Manipulationen berechtigt sind. Auf dieser Basis sind nur eingeschränkte Aussagen über die Integrität im Sinne einer authentischen, korrekten Funktionalität des Daten-Objekts möglich. Legt man demgegenüber die Berechtigungen zur Nutzung von Objekten durch wohl definierte Methoden des Objekts fest, so werden die Nutzungsmöglichkeiten und damit die Manipulationsmöglichkeiten auf die Funktionalität dieser Zugriffsoperationen eingeschränkt. Auf formale Techniken zur Festlegung und Vergabe von Zugriffsrechten wird in Kapitel 6 eingegangen. Die benötigten Mechanismen und Verfahren zur Gewährleistung des Schutzzieles der Datenintegrität gehören zum Bereich der Zugriffskontrolle.

Manipulations-Erkennung

Definition 1.5 fordert, dass unautorisierte Manipulationen nicht unbemerkt bleiben dürfen. Das bedeutet, dass in Umgebungen, in denen eine solche Manipulation nicht a priori verhindert werden kann (z.B. in Netzen), Techniken erforderlich sind, mit deren Hilfe unautorisierte Manipulationen a posteriori erkennbar sind. Auf diese Weise kann verhindert werden, dass unautorisiert manipulierte Daten weiterverarbeitet werden und der mögliche Schaden begrenzt wird. Zur Erkennung von durchgeführten Datenveränderungen werden kryptografisch sichere Hashfunktionen (vgl. Kapitel 8.1) eingesetzt.