3 Grundlagen der Cybersicherheit

3.1 Einführung

Ziel dieses Kapitels ist es, Ihnen einen Überblick über die wichtigsten Aspekte rund um das Thema Cybersicherheit zu geben, damit Sie sich im Dschungel der Begrifflichkeiten zielsicher bewegen können. Dazu führen wir zu Beginn in die grundlegenden Definitionen des übergeordneten Themas der Informationssicherheit ein und grenzen Termini gegeneinander ab. Im zweiten Abschnitt des Kapitels widmen wir uns den sog. Schutzzielen in der IT-Sicherheit und wie sie im Zusammenhang mit der in diesem Buch betrachteten Cybersicherheit stehen. Im dritten Abschnitt wird darauf eingegangen, welche Anforderungen und Standards an die Cybersicherheit in der Apotheke gestellt werden und damit für Sie in der Praxis relevant sind. Im Abschluss des Kapitels adressieren wir diese Anforderungen und legen dar, welche allgemeinen Prozesse und Methoden zur Gewährleistung der Cybersicherheit dadurch in Apotheken berührt sind und wie sie grundsätzlich sichergestellt und verbessert werden kann.

Arbeiten Sie dieses Kapitel durch, um wichtige Grundlagen zu legen, auf die Sie im weiteren Verlauf zurückgreifen können. Grundsätzlich bauen die Folgekapitel auf diesem Wissen auf. Gleichwohl können Sie die Inhalte dieses Abschnitts auch überfliegen, um sich ins Thema einzufinden, und dieses Kapitel im Anschluss als Quelle für technisch-methodische Details zu nutzen, sobald Sie diese zum besseren Verständnis benötigen.

3.2 Abgrenzung und Definition von grundlegenden Begriffen

Im wissenschaftlichen Diskurs und der einschlägigen Literatur existiert leider keine einheitliche Begriffsbildung, wenn über die Themen Informationssicherheit, IT-Sicherheit, Datensicherheit, Cybersicherheit oder Datenschutz diskutiert wird. Vielfach werden diese Termini auch synonym verwendet. Da wir uns für die vorliegende Abhandlung auf die digitalen sicherheitsrelevanten Aspekte von IT-Systemen konzentrieren wollen, erfordert dies im ersten Schritt eine Abgrenzung von einigen Begrifflichkeiten.

3.2.1 Definition von IT-System, Information und Datenobjekt

Ein **IT-System** stellt ein dynamisches technisches System aus miteinander in Verbindung stehenden Komponenten (Hardware, Software, Netzwerk etc.) dar, das gemeinsam Datenobjekte und Informationen sammelt, verarbeitet, speichert und verteilt. In Kombination mit dem Menschen als Nutzer des Systems bildet es ein sog. soziotechnisches System, in dem die Sicherheit nicht ausschließlich durch technische Maßnahmen gewährleistet werden kann. Vielmehr erfordert es die Einbettung von Informationssicherheitsmaßnahmen in die unternehmerische Realität, die Berücksichtigung von gesetzlichen Regelungen, Vorschriften und das unterschiedliche Know-how der Menschen, die es benutzen, um ihre tägliche Arbeit zu verrichten.

Die Kernaufgabe von IT-Systemen ist die Verarbeitung von Informationen zur Unterstützung von Entscheidungsfindungen und Prozessen im betrieblichen Kontext. **Informationen** werden in einem IT-System von Daten oder Datenobjekten, die z. B. in einer Datenbank oder als Datei auf einem Netzlaufwerk vorgehalten werden, abgebildet. Die Information ergibt sich erst durch eine explizite Verarbeitungs- oder Interpretationsvorschrift, die auf Datenobjekte angewendet wird. Um die Information als solche vor unbefugten Zugriffen zu schützen, muss im ersten Schritt immer erst verstanden werden, welche Datenobjekte in der Verarbeitung und Übermittlung der Information beteiligt sind und welche Risikoexposition diese aufweisen. Informationen und Datenobjekte stellen schützenswerte Güter dar.

Datenobjekte wiederum bezeichnen eine bestimmte Menge an Daten, die als Einheit behandelt und geschützt werden müssen. Sie können in unterschiedlichen Medien, Formaten und Systemen vorliegen (Datenbanken, Dateien, E-Mails, Cloud-Speichern oder mobilen Geräten). Dies erfordert demzufolge Sicherheitsstrategien, die auch system- und medienübergreifende Angriffsvektoren adressieren.

3.2.2 Abgrenzung der Begriffe Informationssicherheit, Cybersicherheit, IT-Sicherheit, Datensicherheit und Datenschutz

Der Begriff **Informationssicherheit** ist der umfassendste Begriff und beschreibt den holistischen Schutz aller Arten von Informationen einschließlich Daten, Systeme, Prozesse und Technologien. Synonym wird inzwischen der Begriff der Cybersicherheit verwendet. Der Fokus liegt auf dem Schutz sämtlicher Informationen und Datenobjekten einer Organisation, unabhängig davon, ob sie digital oder physisch vorliegen. Sie umfasst dabei die Aspekte Cybersicherheit, physische Sicherheit, Personalsicherheit sowie Richtlinien und Verfahren, die gemeinsam darauf ausgerichtet sind, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen. Die Zielsetzungen der Informationssicherheit sind einerseits das Management von Risiken im Zusammenhang mit der Verarbeitung, Speicherung, Übertragung und Entsorgung von Informationen und Datenobjekten und andererseits das Ergreifen von adäquaten Maßnahmen im Schadensfall zur Gewährleistung des Geschäftsbetriebes (Business-Continuity-Management). Die dezidierten Schutzziele der Informationssicherheit werden in ▸Kap. 3.3 dargestellt. Auf die für die Apotheke wichtigen und relevanten Maßnahmen zur Prävention und Sicherstellung des Geschäftsbetriebes gehen wir in ▸Kap. 5 ein.

Als ein **informationssicheres System** wird daher ein System definiert, das nur Systemzustände annimmt, die nicht vom Sollzustand abweichen und somit einen unautorisierten Zugriff auf Datenobjekte oder Informationen unterbindet.[29]

29 Vgl. *Eckert*, 2023, S. 6

Die **Cybersicherheit** im engeren Sinn konzentriert sich auf den digitalen Teil der Informationssicherheit. Im Unterschied zur IT-Sicherheit adressiert der Begriff auch das Management von Risiken in vernetzten bzw. verteilten Nicht-IT-Systemen, z. B. dem Internet der Dinge (IoT), SCADA-Systemen zur Prozessüberwachung oder industriellen Steuerungssystemen (ICS). Der Begriff Cybersicherheit wurde eingeführt, da der Anteil der vernetzten Systeme in diesen Bereichen in den vergangenen Jahren exponentiell gestiegen ist und demzufolge auch viele neuartige Risiken und Angriffsvektoren entstanden, die eine Erweiterung und Schärfung des Verständnisses der IT-Sicherheit erforderlich machten. Die Zielsetzung der Cybersicherheit ist demzufolge die Vorbeugung und aktive Abwehr von Cyberbedrohungen, z. B. Hackerangriffe, Malware oder Phishing, um unbefugten Datenzugriff, Datenabfluss oder Datenschutzverletzungen zu verhindern.

Wie im vorherigen Abschnitt erläutert, fokussiert der Begriff **IT-Sicherheit** im Kern auf die Sicherheitsrisiken in IT-Systemen. Dies umfasst die digitalen Anwendungen, Netzwerke und die zugrunde liegende Infrastruktur (z. B. Server, Computer). **Datensicherheit** wird häufig synonym mit der IT-Sicherheit betrachtet, fokussiert sich aber insbesondere auf die Maßnahmen, die sicherstellen sollen, dass keine unautorisierten Zugriffe auf Daten oder Abflüsse der Daten möglich sind. Ein wichtiger Aspekt ist hier die Datensicherung (engl. „backup"), um im Fall von Datenverlust (z. B. nach einem erfolgreichen Angriff durch Ransomware) Sicherungskopien zum Wiederherstellen des funktionsfähigen Zustands (engl. „restore") zur Verfügung zu haben.

Der **Datenschutz** konzentriert sich auf die sog. personenbezogenen Daten und bildet damit nur eine wichtige und besonders schützenswerte Teilmenge an Daten, die von der Informationssicherheit insgesamt umschlossen werden, ab. Der Datenschutz und seine rechtlichen Grundlagen werden in ▸Kap. 2.4 genauer thematisiert.

3.2.3 Informationssicherheits-Managementsystem (ISMS)

Ein ISMS stellt ein Rahmenwerk zur systematischen Verwaltung von Informationssicherheit in einer Organisation dar. Es umfasst eine Reihe von Prozessen, Richtlinien, Verfahren und Tools, die darauf abzielen, die Schutzziele der Informationssicherheit zu gewährleisten. Ein ISMS kann je nach Organisationsgröße nach unterschiedlichen Standards ausgelegt und zertifiziert werden (z. B. nach dem BSI-Grundschutz, der ISIS 12 oder der ISO 27001). Im Kern wird im ISMS geregelt, worauf sich das Rahmenwerk bezieht (Festlegung des Geltungsbereichs), welche Sicherheitsrisiken bestehen, wie diese identifiziert und bewertet werden, wie Risiken überwacht, kontrolliert und abgebaut werden sowie wie kontinuierliche Verbesserungen erreicht werden können.

3.2.4 Abgrenzung von Identifizierung, Authentifizierung und Autorisierung

Die **Identifizierung** beschreibt den Prozess, eine Entität, wie eine Person, ein Gerät oder System, eindeutig zu bestimmen und im zweiten Schritt zu authentifizieren. Die Identifizierung kann durch unterschiedliche Verfahren ermöglicht werden. Die am häufigsten verwendete Methode außerhalb der IT ist das Vorzeigen des Ausweises und der Abgleich mit dem Gesicht oder der Unterschrift. In IT-Systemen ist es die Identifizierung mittels Benutzername und Passwort. Es sind aber auch Verfahren wie Smart Cards und Tokens oder eine biometrische Authentifizierung (z. B. via Fingerabdruck- oder Iris-Scan) denkbar. Werden mehrere Verfahren kombiniert, wird von Multi-Faktor-Authentifizierung gesprochen.

Im Prozess der **Authentifizierung** wird für eine Entität (z. B. ein Benutzer) überprüft, ob die Zugangsdaten (engl. „credentials“) zur vorliegenden Identität passen. In Software-Anwendungen werden hierzu häufig sog. Identity-and-Access-Management(IAM)-Lösungen benutzt, die in ihrer Datenbank für jede Entität ein oder mehrere credentials hinterlegt haben. Sie spielen im Kontext der Informationssicherheit eine bedeutende Rolle und sollten einem erhöhten Schutzbedarf unterliegen, da ein erfolgreicher Angriff auf die Daten zur Authentifizierung einem Angreifer erlaubt, Zugriff auf das System unter anderer Identität zu erhalten.

Der Prozess der **Autorisierung** schließt sich an die Authentifizierung an und bestimmt für eine Entität, welche Berechtigungen/Rechte sie im betrachteten System hat. Diese Zuweisung von Rechten kann z. B. anhand von Rollen (RBAC), Attributen (ABAC) oder Zugriffskontrolllisten (ACL) festgelegt werden.

3.2.5 Definition von Bedrohung und Schwachstelle

In der Informationssicherheit bezeichnet der Begriff **Bedrohung** (engl. „threat“) ein potenzielles Risiko für die Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und stellt damit ein potenzielles Ereignis dar, das bei Eintritt einen Schaden verursacht. Bedrohungen in der Informationssicherheit können von unterschiedlichen Quellen ausgehen:

- externe Angreifer wie Hacker, Cyberkriminelle oder staatlich gesponserte Akteure,
- interne Bedrohungen z. B. durch böswillige Mitarbeiter oder unabsichtliche Fehler von Mitarbeitern,
- natürliche oder unbeabsichtigte Ereignisse wie Brände, Überschwemmungen, technisches Versagen oder Stromausfälle.

Eine **Schwachstelle** (engl. „vulnerability“) stellt eine Schwäche in einem IT-System, einem Netzwerk oder einer Anwendung dar, die von Angreifern ausgenutzt werden kann, um unbefugten Zugriff zu erlangen, Daten zu stehlen oder Schaden anzurichten. Eine Schwachstelle ermöglicht also unter Umständen, dass eine Bedrohung eintreten und ein Schaden entstehen kann. Schwachstellen können dabei auf unterschiedliche Arten entstehen:

- durch Fehler in der Software oder Hardware, die es Angreifern ermöglichen, Schadcodes auszuführen oder Systeme zu kompromittieren,
- durch Fehlkonfigurationen von Systemen oder Netzwerken, die unbefugten Zugriff ermöglichen oder Sicherheitslücken offenlegen,
- durch mangelnde Sicherheitsmaßnahmen und -prozesse, z. B. schwache Passwörter, unzureichende Zugangskontrollen oder fehlende Verschlüsselung,
- durch menschliches Versagen, z. B. das Öffnen von Phishing-E-Mails oder das unbeabsichtigte Teilen vertraulicher Informationen.

Im Umgang mit Schwachstellen ist es einerseits wichtig zu verstehen, dass sie nicht statischer Natur sind, sondern dass über die Zeit immer wieder neue Schwachstellen auftreten, da sich insbesondere die Softwaresysteme ebenfalls kontinuierlich weiterentwickeln. Andererseits können Schwachstellen mittels regelmäßiger Sicherheitsaudits und/oder Penetrationstests identifiziert, bewertet und behoben werden.

3.3 Schutzziele in der Informationssicherheit

Das Konzept der Schutzziele besteht seit Ende der 1980er-Jahre. Es spielte zunächst eine wesentliche Rolle bei der Herstellung von Datensicherheit für Informationstechnik.[30] Anfang 2008 formulierte das Bundesverfassungsgericht unter Rückgriff auf zwei dieser Schutzziele das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und legte damit die Basis für die Propagierung in die Gesellschaft und in das Rechtswesen.

Im Kontext der Informationssicherheit beschreibt der Begriff „Schutzziel" die wichtigsten Prinzipien und Konzepte zur Sicherstellung eines autorisierten Zugriffs auf die Informationen und Datenobjekte. Daraus können die wichtigsten Anforderungen für die Implementierung von Sicherheitsmaßnahmen abgeleitet werden. Sie stellen einen wesentlichen Bestandteil des ISMS dar.

In der Literatur wird häufig die sog. CIA-Triade als konzeptionelle Grundlage zur Klassifizierung von **Schutzzielen** in IT-Systemen genannt. In diesem Konzept, welches auch dem IT-Grundschutz zugrunde liegt, wird insbesondere auf die **Informationsvertraulichkeit** (engl. „confidentiality"), **Datenintegrität** (engl. „integrity") und **Verfügbarkeit** (engl. „availability") als Schutzziele abgestellt (Abb. 3.1).

Wir nutzen in dieser Abhandlung eine Erweiterung der „CIA-Triade" um die Schutzziele **Authentizität** (engl. „authenticity") und **Nichtabstreitbarkeit** (engl. „non-repudiation"), wie sie z. B. Eckert vorschlägt[31], da sie die Anforderungen an den Umgang mit sensiblen, personenbezogenen Daten, wie sie in der Apotheke im täglichen Geschäft kontinuierlich auftreten, besser abdeckt. Diese Kombinationen aus den genannten fünf Schutzzielen werden auch als Grundsäulen der IT-Sicherheit bezeichnet.[32] In der Folge werden die Schutzziele inhaltlich vorgestellt und erläutert, wie das vorliegende Niveau gemessen und überwacht werden kann.

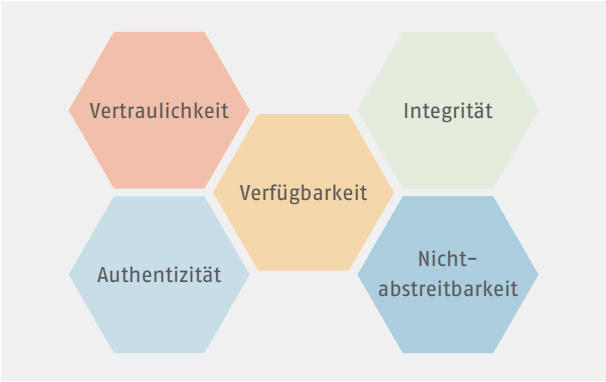

Abb. 3.1 Schutzziele der Informationssicherheit

30 Vgl. *Voyduck und Kent*, 1983, S. 138
31 Vgl. *Eckert*, 2023 (S. 7 ff.)
32 Vgl. *Hellmann* 2023, S. 7 f.

3.3.1 Vertraulichkeit

Sie stellt sicher, dass sensible oder vertrauliche Informationen in der Apotheke vor unbefugtem Zugriff, Offenlegung, Veränderung oder Zerstörung geschützt sind. Vertraulichkeit gewährleistet, dass Informationen nur an autorisierte Personen, Systeme oder Prozesse weitergegeben werden, die die notwendigen Berechtigungen und Zugriffsrechte haben, sodass diese nicht in die falschen Hände geraten und missbraucht werden können. Eine wichtige Voraussetzung zur Erreichung von Vertraulichkeit sind beispielsweise kryptografische Maßnahmen zur Absicherung der Kommunikation. Einige beispielhafte Metriken umfassen:

- Die **Anzahl der Sicherheitsverletzungen,** die zu Verstößen gegen die Vertraulichkeit führen. Eine geringe Anzahl von Sicherheitsverletzungen deutet auf ein hohes Niveau von Vertraulichkeit hin.
- Die **Anzahl der nicht autorisierten Zugriffe:** Eine geringe Anzahl von nicht autorisierten Zugriffen deutet auf ein hohes Niveau von Vertraulichkeit hin.
- Die **Anzahl der Zugriffe auf vertrauliche Informationen:** Eine geringe Anzahl von Zugriffen deutet auf ein hohes Niveau von Vertraulichkeit hin.
- Die **Anzahl der Zugriffe auf vertrauliche Informationen durch unbefugte Benutzer:** Eine geringe Anzahl von Zugriffen durch unbefugte Benutzer deutet auf ein hohes Niveau von Vertraulichkeit hin.
- Die **Zeit, die benötigt wird, um eine Sicherheitsverletzung zu erkennen und zu beheben** (siehe MTTR): Eine schnelle Erkennung und Behebung von Sicherheitsverletzungen deuten auf ein hohes Niveau von Vertraulichkeit hin.
- Die **Anzahl der Schulungen und Sensibilisierungsmaßnahmen:** Eine hohe Anzahl von Schulungen und Sensibilisierungsmaßnahmen deutet auf ein hohes Niveau von Vertraulichkeit hin.

3.3.2 Integrität

Die Integrität beschreibt die Sicherstellung der Korrektheit, Vollständigkeit und Unversehrtheit von Informationen und Daten in einem System. In der Apotheke ist sie essenziell, da Kunden, Partner und Mitarbeiter auf die Korrektheit der sensiblen Daten angewiesen sind. Eine absichtliche oder unabsichtliche Manipulation von Daten und damit eine Verletzung der Integrität kann allerdings in der Regel nur a posteriori festgestellt werden. Zur Überprüfung und der Rekonstruktion der Veränderungen von Daten kommen häufig Prüfsummen, Richtungsindikatoren oder auch Sequenznummern zum Einsatz. Folgende Metriken können zur Messung der Integrität herangezogen werden.

- **Anzahl der Integritätsverletzungen:** misst die Verletzungen der Integrität von Daten in einem System über die Zeit. Je geringer die Anzahl von Integritätsverletzungen, desto höher die Integrität des Systems.
- **Fehlerrate:** Die Fehlerrate ist eine Metrik, die die Anzahl der fehlerhaften Daten im Verhältnis zur Gesamtzahl der Daten misst. Eine niedrige Fehlerrate bedeutet, dass die Daten in der Regel korrekt sind und die Integrität der Daten hoch ist.
- **Änderungsrate:** Gemessen wird die Anzahl der Änderungen an Daten im Verhältnis zur Gesamtzahl der Daten in einem System. Je niedriger die Änderungsrate, desto stabiler das System und desto höher die Integrität der Daten.

- **Hashwert-Übereinstimmung:** Verglichen wird, ob die Hashwerte vor und nach der Übertragung oder Speicherung von Daten übereinstimmen. Wenn keine Übereinstimmung vorliegt, handelt es sich um eine Verletzung der Integrität.
- **Anzahl der Audit-Trails:** Die Anzahl der Audit-Trails ist eine Metrik, die die Anzahl der aufgezeichneten Aktivitäten von Benutzern und Systemen misst. Eine hohe Anzahl von Audit-Trails bedeutet, dass die Integrität der Daten überwacht und überprüft wird.

3.3.3 Verfügbarkeit

Die Verfügbarkeit bezieht sich auf den Zugang und Zugriff zu Informationen und Systemen, sodass autorisierte Benutzer diese ohne Beeinträchtigungen und Unterbrechungen jederzeit, von überall und mit jedem Gerät nutzen können. Eine hohe Verfügbarkeit ist die Grundvoraussetzung für die Gewährleistung einer hohen Produktivität und die Sicherstellung der Geschäftskontinuität von Organisationen. Zur Abgrenzung und Bestimmung der Anforderungen der Verfügbarkeit an IT-Systeme können zwei Ansätze herangezogen und kombiniert werden: einerseits die Verfügbarkeitsklassifikation (Availability Environment Classification, AEC) der Harvard Research Group (HRG) und andererseits das 9er-System des BSI.

Die Klassifikation des AEC stützt sich auf zwei Dimensionen und erzeugt 6 unterschiedliche Klassen (AEC0 bis AEC5).[33] Die erste, quantitative Dimension stellt die maximal akzeptable Nichtverfügbarkeit eines Systems dar. Die zweite Dimension ist qualitativer Natur und bewertet die Möglichkeiten der Wiederherstellung von Transaktionen, Datenobjekten und Informationen während einer Nichtverfügbarkeit.

- **Klasse 1 (AEC0 = conventional)**: umschließt Systeme, die längere Ausfallzeiten tolerieren können. Daten können verloren gehen oder verfälscht werden. Beispiele hierfür sind Archivierungssysteme oder Sicherungssysteme.
- **Klasse 2 (AEC1 = highly reliable)**: ist für Systeme gedacht, die Ausfallzeiten von mehreren Stunden pro Jahr tolerieren können. Die Daten können allerdings aufgrund redundanter Datenspeicherung und unterbrochener Transaktionen durch Rekonstruktion via Logdateien wiederhergestellt werden. Beispiele für Systeme, die in diese Klasse fallen können, sind E-Mail-Systeme, Dateiserver und Webserver.
- **Klasse 3 (AEC2 = high availability)**: beherbergt Systeme mit minimalen akzeptablen Unterbrechungszeiten. Diese werden hier definiert als Ausfallzeiten von maximal mehreren Minuten pro Monat. Typische Systeme dieser Klasse stellen Transaktionsverarbeitungssysteme, Onlinebestellsysteme und Reservierungssysteme dar.
- **Klasse 4 (AEC3 = fault resilient)**: umfasst Systeme, die Ausfallzeiten von mehreren Sekunden pro Monat verkraften können (sog. unterbrechungsfreier Betrieb). Beispiele für Systeme, die in diese Klasse fallen können, sind Echtzeit-Kontrollsysteme, Finanzhandelssysteme und Notfallsysteme.
- **Klasse 5 (AEC4 = fault tolerant)**: ist für Systeme gedacht, die aufgrund der Kritikalität der Geschäftsprozesse eine kontinuierliche Verfügbarkeit erfordern, sodass sie 24h am Tag, 7 Tage die Woche, 365 Tage im Jahre erreichbar und funktionsfähig sind.
- **Klasse 6 (AEC5 = disaster tolerant)**: beschreibt Systeme, die unter allen Umständen, auch im Fall einer Katastrophe (Erdbeben, Überflutung, Stromausfall über längere Zeiten oder Cyberangriff), verfügbar und ohne Funktionseinschränkung nutzbar sind.

33 Vgl. *Harvard Research Group*, 2001

Tab. 3.1 Vergleich der unterschiedlichen Verfügbarkeitsklassifikationen (VK) nach AEC und BSI

VK nach AEC	Verfügbarkeit nach BSI-9er-System	Max. Ausfallzeit pro Jahr
AEC0	Ohne zugesicherte Verfügbarkeit	
AEC 1	99 %	< 3 Tage 15 Stunden 40 Minuten
AEC 2	99,9 %	< 8 Stunden 46 Minuten
AEC 3	99,99 %	< 53 Minuten
AEC 4	99,999 %	< 6 Minuten
AEC 5	99,9999 % (disaster tolerant)	Weniger als 1 Minute

Dies setzt insbesondere redundante Komponenten im System voraus. In diese Kategorie fallen z. B. lebenswichtige Systeme in Krankenhäusern oder in der Elektrizitätsübertragung.

Das Klassifikationssystem des BSI zielt insbesondere auf die quantitative Verfügbarkeit von Systemen im Monats- und/oder Jahresmittel ab. In Tab. 3.1 sind beide Klassifikationen gegenübergestellt.

Häufig wird von sog. **hochverfügbaren Systemen** gesprochen, wenn einerseits die Anforderungen der Klasse 3 der AEC-Kategorisierung und andererseits eine quantitative Verfügbarkeit von 99,9 % erreicht sind.

Neben der Sicht auf die reine Verfügbarkeit eines singulären IT-Systems oder Prozesses sollten weitere Metriken zur Bewertung der Zuverlässigkeit herangezogen werden.

- Mean Time Between Failure (MTBF): gibt die mittlere ausfallfreie Zeit eines Systems/Prozesses zwischen zwei Ausfällen an.
- Mean Time To Repair/Recovery (MTTR): beschreibt die durchschnittliche Zeit, die benötigt wird, um das System/den Prozess nach einem Ausfall wieder in den betriebsbereiten und fehlerfreien Zustand zu versetzen.

3.3.4 Authentizität

Das Schutzziel der Authentizität im Kontext der Informationssicherheit bezieht sich auf die Eigenschaft von Daten, Informationen oder Systemen, dass sie tatsächlich von der angegebenen Quelle bzw. dem Urheber stammen und dass sie nicht verfälscht oder manipuliert wurden, also echt sind. Sie umfasst die drei Eigenschaften der Echtheit, der Überprüfbarkeit und der Vertrauenswürdigkeit.[34]

Es gibt verschiedene Arten von Authentizität, darunter:

- Identitätsauthentizität bezieht sich auf die Fähigkeit, die Identität eines Benutzers oder Systems eindeutig zu bestimmen und zu überprüfen.
- Datenauthentizität bezieht sich auf die Fähigkeit, die Integrität und Echtheit von Daten zu überprüfen und sicherzustellen, dass sie nicht verfälscht oder manipuliert wurden.
- Systemauthentizität bezieht sich auf die Fähigkeit, die Integrität und Echtheit von Systemen zu überprüfen und sicherzustellen, dass sie nicht kompromittiert wurden.

34 Vgl. *Porath*, 2020, S. 43

Ist die Authentizität einer Person oder eines Systems überprüft und ist sie/es auch durch ein Berechtigungskonzept berechtigt, also autorisiert, dann sollte ein funktionsfähiges System Zugriff auf die Informationen oder Datenobjekte gewähren. Ist dies der Fall, handelt es sich um ein verfügbares System.

Authentizität kann nicht direkt gemessen werden, sondern nur durch die Kombination von Authentifizierung, Integritätsprüfung, Zugriffskontrolle, Überwachung und Auditing gewährleistet werden.

3.3.5 Nichtabstreitbarkeit

Nichtabstreitbarkeit oder auch Verbindlichkeit bezieht sich auf die Fähigkeit, die Urheberschaft und Herkunft von Informationen oder Transaktionen eindeutig zuzuordnen und gegenüber Dritten zu beweisen. Eine Person oder ein System ist demzufolge nicht in der Lage, eine Aktion oder Transaktion abzustreiten. So kann sichergestellt werden, dass Informationsübermittlung und -verarbeitung rechtlich und vertraglich bindend ausgestaltet werden können. Die Basis dafür legen z. B. elektronische Signaturen. Im Kontext der Nichabstreitbarkeit kann zwischen der Herkunft und dem Erhalt von Datenobjekten und Informationen unterschieden werden.[35] So soll es sowohl dem Absender als auch dem Empfänger unmöglich gemacht werden, den Versand bzw. den Erhalt der Information oder des Datenobjektes abzustreiten.

Die Nichtabstreitbarkeit ist ein qualitatives Schutzziel und kann daher nicht direkt gemessen werden. Allerdings kann die Wirksamkeit der eingesetzten Mechanismen überprüft werden:

- Durch die Prüfung von Protokollen, die die Aktionen oder Transaktionen im IT-System aufzeichnen, kann sichergestellt werden, dass die Protokolle die notwendigen Informationen enthalten, um die Urheberschaft eindeutig zuzuordnen und zu beweisen.
- Anhand von Simulationen von Angriffen auf die eingesetzten Mechanismen zur Nichtabstreitbarkeit kann sichergestellt werden, dass die Maßnahmen funktionieren und die entsprechenden Resultate liefern.
- Durch die Überprüfung der Implementierung von Mechanismen zur Nichtabstreitbarkeit kann gewährleistet werden, dass die notwendigen Sicherheitsfunktionen enthalten sind.
- Durch Zertifizierungen, die von unabhängigen Dritten ausgestellt wurden, kann überprüft werden, ob die Mechanismen zur Nichtabstreitbarkeit den geltenden Standards und Best Practices entsprechen.

3.3.6 Exkurs: Schutzziele des Datenschutzes

Zusätzlich zu den Schutzzielen der Informationssicherheit, die sich insbesondere auf den funktionssicheren Betrieb von Systemen und Organisationen beziehen, bedarf es weiterer, spezifischer Schutzziele, die die Perspektive der individuell betroffenen Personen gegenüber Organisationen (Unternehmen, Behörden etc.) in Bezug auf den Datenschutz einnehmen. Hierzu dienen drei zusätzliche Schutzziele, die als Schutzziele des Datenschutzes bezeichnet werden.[36]

35 Vgl. *Gadatsch und Mangiapane*, 2017, S. 22

36 Vgl. *Rost*, 2012, S. 355

Transparenz

Das Schutzziel der Transparenz im Kontext des Datenschutzes bezieht sich auf die Notwendigkeit, personenbezogene Daten klar, verständlich und zugänglich darzustellen, damit Betroffene ihre Rechte wahrnehmen (z. B. der Verarbeitung ihrer Daten zustimmen oder dieses verweigern) und die Verarbeitung ihrer Daten überprüfen können. Transparenz ist erforderlich, um sowohl Betroffene als auch Betreiber von IT-Systemen und zuständige Kontrollinstanzen in die Lage zu versetzen zu erkennen, welche Daten für welchen Zweck erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wem die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung gehören.

Zur Umsetzung der Transparenzanforderung können Monitoring-Systeme, Protokollierungen und Dokumentationen eingesetzt werden. Im Rahmen der Umsetzung offenbaren sich oftmals Regelungslücken in der Datenverarbeitung. Transparenz ist letztlich auch eine Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben werden kann.

Intervenierbarkeit

Die Intervenierbarkeit bezieht sich auf die Möglichkeit von Betroffenen und Betreibern von Systemen, die Verarbeitung personenbezogener Daten zu beeinflussen und gegebenenfalls zu ändern oder zu stoppen. Das bedeutet, dass Betroffene die Möglichkeit haben, ihre Einwilligung zur Verarbeitung ihrer Daten jederzeit zu erteilen oder zu widerrufen.

Technisch wird dieses Ziel z. B. durch eine Abfrage in einem Pop-up-Fenster innerhalb einer Softwareanwendung gelöst, bei dem der Nutzer der Verarbeitung seiner Daten temporär über einen Button (An-aus-Knopf) zustimmen kann. Diese Funktionalität ist vergleichbar mit einer rechtlichen Einwilligung, die erteilt oder verweigert werden kann.

Die Intervenierbarkeit ist ein wichtiges Schutzziel im Datenschutz, da es Betroffenen ermöglicht, die Verarbeitung ihrer Daten zu überwachen und zu kontrollieren. Durch die Möglichkeit, die Verarbeitung von Daten zu beeinflussen und gegebenenfalls zu stoppen, können Betroffene sicherstellen, dass ihre Daten korrekt und rechtmäßig verarbeitet werden.

Die Umsetzung des Schutzziels der Intervenierbarkeit erfordert eine klare und transparente Kommunikation mit Betroffenen, zum Beispiel durch die Bereitstellung von Kontaktinformationen für Datenschutzbeauftragte und andere Ansprechpartner. Unternehmen und Organisationen müssen sicherstellen, dass Betroffene ihre Rechte einfach und unkompliziert ausüben können, zum Beispiel durch die Bereitstellung von Onlineformularen oder andere benutzerfreundliche Technologien.

Nichtverkettbarkeit

Das Schutzziel der Nichtverkettbarkeit bezieht sich auf die Anforderung sicherzustellen, dass personenbezogene Daten nur für den Zweck verarbeitet und ausgewertet werden (sog. Zweckbindung), für den sie erhoben wurden, und auf diese Weise eine vertrauensvolle Beziehung zwischen einer Person und einer Organisation zustande kommen kann. Mit anderen Worten: Die Nichtverkettbarkeit ist der technische Ausdruck der Anforderung an Zweckbindung und Zwecktrennung, die als Funktionstrennungen einen wesentlichen Mechanismus zur Umsetzung von Checks und Balancen darstellen.[37]

37 Vgl. *Rost*, 2012, S. 358

Die Umsetzung der Nichtverkettbarkeit erfordert einerseits eine klare Begründung der Erforderlichkeit der Datenverarbeitung und andererseits das Bekenntnis, Datensparsamkeit auszuüben, aber auch eine transparente Kommunikation mit Betroffenen, zum Beispiel durch die Bereitstellung von Informationen darüber, welche Daten erhoben und verarbeitet werden und für welchen Zweck. Darüber hinaus müssen Unternehmen und Organisationen sicherstellen, dass personenbezogene Daten angemessen geschützt werden, zum Beispiel durch die Anwendung von Zugriffsbeschränkungen und anderen Sicherheitsmaßnahmen. Eine sehr wirksame Maßnahme, das Schutzziel zu erreichen, ist die Anonymisierung oder Pseudoanonymisierung der personenbezogenen Daten vor der Datenverarbeitung. Die Nichtverkettbarkeit trägt demzufolge dazu bei, das Vertrauen von Betroffenen in die Verarbeitung ihrer personenbezogenen Daten zu stärken und sicherzustellen, dass ihre Daten korrekt und rechtmäßig verarbeitet werden. Durch die Beachtung der Schutzziele und deren Umsetzung durch Schutzmaßnahmen können Organisationen nachweisen, dass sie ihre Prozesse und Systeme beherrschen und dabei an Fairness orientiert sind, weil sie sich an die Regeln halten.

3.4 Grundlegende Sicherheitstechniken in der Informationssicherheit

Dieser Abschnitt widmet sich den grundlegenden Sicherheitsprinzipien und -techniken. Wir werden uns mit den wichtigsten Strategien befassen, die Sie anwenden können, um Ihre IT-Systeme und sensiblen Daten zu schützen. Doch keine Sorge, unser Ziel ist es, Ihnen diese Konzepte auf eine klare und verständliche Weise näherzubringen. Sie benötigen keine fortgeschrittenen IT-Kenntnisse, um diese Prinzipien zu verstehen.

3.4.1 Sicherheitsprinzipien und -modelle

Zero-Trust-Security-Modell

Das **Zero-Trust-Security-Modell** ist ein Sicherheitsmodell, das davon ausgeht, dass alle Benutzer, Geräte und Netzwerke von vornherein unzuverlässig sind. Der Zugriff auf Ressourcen wird auf Anfragebasis gewährt, anstatt davon auszugehen, dass Benutzer, Geräte oder Netzwerke vertrauenswürdig sind. Es basiert auf folgenden Grundprinzipien:

- **Nie vertrauen, immer überprüfen** (never trust, always verify). Dieses Prinzip beinhaltet die Überprüfung der Identität und Sicherheit von Benutzern, Geräten und Netzwerken, bevor der Zugriff auf Ressourcen gewährt wird. Hierbei können Multi-Faktor-Authentifizierung, Geräte-Sicherheitsprüfungen und andere Sicherheitsmaßnahmen zum Einsatz kommen.
- Das Prinzip der **geringsten Privilegien** (least privilege) besagt, dass Benutzern, Geräten und Netzwerken nur das Mindestzugriffsniveau gewährt werden sollte, das für die Ausführung ihrer Aufgaben erforderlich ist. Dies kann dazu beitragen, das Risiko unbefugten Zugriffs oder von Datenverletzungen zu verringern.
- Als **Mikrosegmentierung** wird die Aufteilung eines Netzwerks in kleinere, isolierte Segmente bezeichnet, um das Risiko von Seitwärtsbewegungen (Beschränkung auf einen kleinen Teil des Netzwerkes) von Angreifern zu verringern. Dadurch kann das Ausmaß eines Sicherheitsverstoßes begrenzt werden.

- **Kontinuierliches Monitoring** der Systemlandschaft. Ziel ist die kontinuierliche Überwachung und Analyse des Netzwerkverkehrs sowie des Benutzerverhaltens, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Dies kann z. B. die Verwendung von Intrusion-Detection-Prävention-Systemen und Sicherheitsinformations- und Ereignismanagement-Systemen (SIEM) umfassen.
- **Automatisierung und Orchestrierung**: Mittels der Automatisierung von Sicherheitsprozessen können die Effizienz verbessert und das Risiko menschlicher Fehler reduziert werden. Dabei unterstützen Sicherheitsautomatisierungs- und Orchestrierungstools, die Aufgaben wie Bedrohungserkennung, Incident Response und Compliance-Berichterstattung automatisieren.

Privacy by Design

Privacy by Design ist ein proaktiver Ansatz zum Schutz personenbezogener Daten, bei dem Datenschutzaspekte in die Gestaltung und Entwicklung von Informationssystemen (IT-Systemen, Anwendungen, Netzwerken), Prozessen und Produkten integriert werden. Er basiert auf der Idee, dass der Datenschutz in den Kern der Arbeitsabläufe einer Organisation eingebettet sein sollte und nicht nur ein nachträglicher Gedanke. Der Grundsatz des „eingebauten Datenschutzes" umfasst die folgenden sieben Prinzipien[38]:

1. **Proactive, not reactive**: Privacy by Design antizipiert und verhindert Datenschutzprobleme, anstatt auf sie zu reagieren, nachdem sie bereits aufgetreten sind.
2. **Privacy by Default**: Persönliche Daten sollten im Standardzustand eines Informationssystems, eines Prozesses oder eines Produkts automatisch geschützt sein.
3. **Privacy embedded into design**: Der Datenschutz sollte in das Design und die Architektur von Informationssystemen, -prozessen und -produkten integriert werden, anstatt nachträglich hinzugefügt zu werden.
4. **Full function**: Datenschutz durch Design sollte die Funktionalität von Informationssystemen, -prozessen und -produkten nicht beeinträchtigen.
5. **End-to-End-Security**: Personenbezogene Daten sollten während des gesamten Lebenszyklus eines Informationssystems, eines Prozesses oder eines Produkts geschützt werden, von der Erfassung bis zur Entsorgung (Ende-zu-Ende-Sicherheit).
6. **Visibility and transparency**: Die Datenschutzmaßnahmen und -praktiken einer Organisation sollten transparent und für den Einzelnen sichtbar sein.
7. **Respect for user privacy**: Die Privatsphäre des Einzelnen sollte jederzeit respektiert und geschützt werden.

Segregation of Duties

Das Prinzip der Aufgabentrennung (**Segregation of Duties**, SoD) ist ein grundlegendes Sicherheitskonzept, bei dem Aufgaben und Verantwortlichkeiten auf mehrere Personen aufgeteilt werden, um das Risiko von Betrug, Fehlern und anderen Sicherheitsbedrohungen zu verringern. Dies wird erreicht, indem verschiedene Aspekte einer Aufgabe oder eines Prozesses auf mehrere Personen aufgeteilt werden, wodurch es für eine einzelne Person schwieriger wird, unbefugte oder böswillige Aktivitäten auszuführen. Im Kontext einer Apotheke kann das Prinzip der Aufgabentrennung am Beispiel der Warenannahme, Ausgabe und Inventur erklärt werden. Werden diese Tätigkeiten von ein und derselben

38 Vgl. *Rost und Bock,* 2011, S. 31

Person durchgeführt, können betrügerische oder fehlerhafte Tätigkeiten ohne Aufsicht oder Überprüfung durchgeführt werden. Daher ist es empfehlenswert, insbesondere bei geschäftskritischen Prozessen, das Prinzip der Aufgabentrennung anzuwenden.

Need-to-know-Prinzip

Das **Need-to-know-Prinzip** (NtK) umfasst alle Maßnahmen, die getroffen werden sollten, um den Zugang zu sensiblen Informationen und Ressourcen auf diejenigen Personen zu beschränken, die wirklich einen legitimen Bedarf daran haben. Das heißt, das Risiko von Sicherheitsverletzungen kann signifikant verringert werden, indem die Anzahl der Personen, die Zugang zu sensiblen Informationen und Ressourcen haben, begrenzt wird. In der Apotheke wäre eine Maßnahme beispielsweise, dass nur ein beschränkter Personenkreis Zugriff auf das System zur Medikamentenausgabe erhält. Eine weitere denkbare Maßnahme ist, alle patientenbezogenen Daten zu verschlüsseln und den Zugang zu den Entschlüsselungsverfahren nur einem begrenzten Teil der Mitarbeitenden zur Verfügung zu stellen.

Defense in Depth

Ein weiteres wichtiges Prinzip in der Informationssicherheit ist der sog. **Defense-in-Depth**-Ansatz (DiD). Er adressiert das Problem, dass keine einzelne Sicherheitskontrolle fehlerfrei und narrensicher ist. Daher beinhaltet er die Implementierung mehrerer Schichten von Sicherheitskontrollen zum Schutz vor Bedrohungen und zur Verringerung des Risikos von Sicherheitsverletzungen. Das DiD-Prinzip kann in verschiedenen Kontexten angewendet werden, z. B. bei der Netzwerksicherheit, der Anwendungssicherheit und der physischen Sicherheit.

Fail-Safe Defaults

Das Prinzip der ausfallsicheren Vorgaben bzw. Voreinstellungen (engl. „Fail-Safe Defaults“, FSD) zielt darauf ab, die Konfiguration von Systemen und Anwendungen mit sicheren Standardeinstellungen auszustatten, um das Risiko von Sicherheitsverletzungen zu verringern. Es basiert auf der Erkenntnis, dass viele Sicherheitsverletzungen auf falsch konfigurierte Systeme und Anwendungen zurückzuführen sind. Die Berücksichtigung von Fail-Safe Defaults kann im Falle eines Systemausfalls oder -fehlers unbefugten Zugriff oder Datenverletzungen verhindern. Ein technisches Beispiel zur praktischen Umsetzung ist, Ihre Firewall auf eine Weise zu konfigurieren, dass sie als Voreinstellung keine Verbindungen von außerhalb des Netzwerkes zulässt (Default). Im zweiten Schritt werden für notwendige, vertrauenswürdige Verbindungen Ausnahmen eingerichtet.

Datensparsamkeit

Das Prinzip der **Datensparsamkeit** (engl. „Data Minimization“, DM) basiert auf dem Konzept, dass die Erfassung, Verarbeitung und Speicherung der minimalen Datenmenge, die zur Erfüllung eines bestimmten Zwecks erforderlich ist, dazu beitragen können, das Risiko von Sicherheitsverletzungen zu verringern. Die Umsetzung des DM-Prinzips kann die allgemeine Sicherheitslage einer Organisation verbessern und sensible Daten vor unbefugtem Zugriff schützen.