

Fernstudium
Industrial Engineering
Produktions- und Betriebstechnik

Kurseinheit 98

Datensicherheit und Datenschutz

Prof. Dr. J. Rauchfuß

Fernstudieninstitut

1 Datenschutz

Lernziele und Überblick

In dieser Lerneinheit sollen die grundlegenden Begriffe und Definitionen zum Datenschutz und dem Komplex der Datensicherheit eingeführt werden. Die Aufteilung in Datenschutz und Datensicherheit zieht sich durch den Inhalt der gesamten Kurseinheit. Sie ist notwendig, um die vielfältigen Vorschriften und Vorgaben zum Datenschutz entsprechend berücksichtigen zu können.

1.1 Einführung

1.1.1 Begriffsbestimmung - Datenschutz, Datensicherung, Datensicherheit

Datenschutz

Ist der Schutz von Daten vor Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung, aus welchen Motiven auch immer. Im engeren Sinne (in der Gesetzgebung) sind damit nur personenbezogene Daten gemeint, im Allgemeinen werden damit aber alle Daten gemeint, die irgendwo erhoben, gesammelt oder gespeichert werden. Der notwendige Schutz bezieht sich auch auf die Integrität eines Daten verarbeitenden Systems als auch der Schutz vor Fehlern und Folgefehlern.

Datensicherung

Ist die Gesamtheit aller organisatorischen und technischen Vorsorgemaßnahmen gegen Verlust, Fälschung und unberechtigten Zugriff auf Grund von Katastrophen, technischen Ursachen, menschlichem Versagen oder mutwilligen Eingriffen.

Datensicherheit

Ist der angestrebte Zustand, der durch Maßnahmen der Datensicherung erreicht worden ist, aber wegen der Beschränkung aller Maßnahmen nie eine 100%ige Sicherheit geschaffen werden kann.



Abb. 1.1: Übersicht zum Verhältnis Datenschutz, Datensicherheit, Datensicherung

Um die Datensicherheit zu gewährleisten werden Schutzziele definiert, die im Folgenden erläutert werden sollen.

Datensicherheit – Schutzziele

Ausgehend davon, dass die Informationen bzw. Daten zu schützen sind, ist der Zugriff auf diese zu beschränken und zu kontrollieren. Die entsprechenden Schutzziele sind die Vertraulichkeit und die Integrität. Die auf die Daten zugreifenden Personen oder Prozesse müssen eindeutig identifiziert und ihre Identität muss verifiziert sein, d. h. ihre Authentizität ist festgestellt. Wurde die Person oder Prozess eindeutig identifiziert und die Berechtigung bestätigt, dann sollte das System diesen Zugriff auch ermöglichen, d. h. die Verfügbarkeit ist zu gewährleisten. Ist ein Zugriff auf Daten erfolgt oder eine Aktion durchgeführt worden, ist es auch im Nachhinein notwendig, die Urheberschaft des Zugriffs bzw. der Aktion eindeutig zuordenbar zu gestalten (Zuordenbarkeit).

1.1.2 Begriffsbestimmung – Authentizität, Datenintegrität, Vertraulichkeit

Authentizität

Unter Authentizität (engl.: authenticity) eines Objektes soll die Echtheit und Glaubwürdigkeit eines Objektes verstanden werden, die anhand einer eindeutigen Identifizierung festgestellt worden ist. Die Authentizität eines Objektes wird durch Maßnahmen zur Authentifizierung nachgewiesen. Dabei muss nachgewiesen werden, dass eine behauptete Identität eines Objektes mit dessen charakteristischen Eigenschaften übereinstimmt.

In bekannten Systemen wird eine Authentifikation eines Objektes über die Bestimmung eines Nutzers vorgenommen. Die Identifikation erfolgt über Nutzernamen, die in einem eindeutigen Vergabeverfahren erstellt worden sind. Die charakteristischen Eigenschaften für einen Nutzer sind z. B. ein Passwort, dessen Kenntnis der Nutzer durch Eingabe nachweisen muss. Das Eingeben eines Passwortes kann ersetzt oder ergänzt werden, indem biometrische Merkmale des Nutzers (Fingerabdruck, Stimme, Gesicht o.ä.) eingesetzt werden. Wichtig hierbei ist die Sicherung der Eindeutigkeit der charakteristischen Eigenschaften.

Datenintegrität

Die Datenintegrität ist gewährleistet, wenn es nicht gelingt, die zu schützenden Daten unautorisiert und unbemerkt zu verändern. Die Sicherung der Datenintegrität ist verknüpft mit der Festlegung von Rechten zur Nutzung von Daten z. B. durch Lese- oder Schreibrechte für Dateien. Die Mechanismen und Verfahren zur Gewährleistung der Datenintegrität gehört zum Bereich der Zugriffskontrolle.

Ein besonderes Augenmerk ist bei der Sicherung der Datenintegrität darauf zu richten, dass unautorisierte Manipulationen nicht unentdeckt bleiben dürfen. Dies bedeutet, dass in Umgebungen, wo ein Zugriff nicht von Vornherein verhindert werden kann, Maßnahmen notwendig sind, mit denen unautorisierte Manipulationen erkannt werden können. Eine mögliche Maßnahme ist die Anwendung von kryptografischen Verfahren.

Vertraulichkeit

Mit Vertraulichkeit ist der Schutz der gespeicherten oder übermittelten Daten vor unberechtigter Einsicht zu verstehen. Zur Sicherung der Vertraulichkeit von Daten ist die Festlegung von Zugriffsrechten und der Kontrolle der Zugriffe erforderlich, um sicherzustellen, dass nur autorisierte Nutzer Kenntnis von den Informationen erlangen.

Die Anforderungen an die Informationsvertraulichkeit werden durch Verschlüsselungstechniken gewährleistet. Das Ziel besteht hierbei darin, die Daten so umzuwandeln, dass unautorisierte Zugriffe es nicht erlauben, die Daten sinnvoll zu interpretieren, ohne die Umwandlungsvorschrift zu kennen. Dies bedeutet, dass zur Sicherung der Vertraulichkeit zusätzliche Maßnahmen notwendig sind, die über das reine Regeln von Zugriffsrechten hinausgehen.

1.1.3 Begriffsbestimmung – Verfügbarkeit, Zurechenbarkeit, Anonymisierung

Verfügbarkeit

Um die zugewiesenen Zugriffsrechte wahrnehmen zu können, ist es notwendig, dass das System die entsprechenden Leistungen zur Verfügung stehen. Allgemein lässt sich formulieren, dass das System die Verfügbarkeit gewährleistet, wenn authentifizierte und autorisierte Nutzer in der Wahrnehmung ihrer Rechte nicht unautorisiert beeinträchtigt werden. Zur Sicherung der Verfügbarkeit sind Maßnahmen, wie z. B. die Vergabe von Quoten für Systemressourcen, vorzusehen.

Zurechenbarkeit

Als Zurechenbarkeit oder Verbindlichkeit wird die eindeutige Zuordenbarkeit des Urhebers oder Verantwortlichen für die erhobenen, gespeicherten oder übermittelten Daten verstanden. Die Anforderungen an die Zurechenbarkeit lassen sich durch den Einsatz digitaler Signaturen erfüllen.

Anonymisierung und Pseudomisierung

Unter der Anonymisierung versteht man das Verändern personenbezogener Daten so, dass die Angaben über persönliche oder sachliche Verhältnisse nicht mehr zugeordnet werden können.

Die schwächere Form der Anonymisierung stellt die Pseudomisierung dar. Dabei werden die personenbezogenen Daten durch eine Zuordnungsvorschrift (Verwendung von Pseudonymen) so verändert, dass die Angaben über persönliche oder sachliche Verhältnisse nicht mehr den natürlichen Personen zugeordnet werden kann.

Auf diese Aspekte im Zusammenhang mit der ärztlichen Tätigkeit wird im nächsten Kapitel eingegangen.