Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Datenbanken

Vorlesungsskript für das 3. Semester

Studiengang Internationale Medieninformatik

8. Datenschutz und Datensicherheit in Datenbanksystemen

Dozent: M. Sc. Burak Boyaci

Version: 09.12.2025

Wintersemester 25/26

12

Datenschutz und Datensicherheit

Kapitelübersicht

12.1 Datenschutz

In Datenbanken werden verschiedenste personenbezogene Daten gespeichert. Ziele der Speicherung dieser Daten sind meist vielfältig. So können die Daten benötigt werden, um Kunden einen Brief zusenden zu können oder auch um bestimmte rechtliche Vorgaben erfüllen zu können. Generell dürfen Daten in diesem Zusammenhang jedoch nur unter bestimmten Voraussetzungen erhoben und dauerhaft gespeichert werden. Diese Gesetze und Regeln sind auf nationaler Ebene im Bundesdatenschutzgesetz (BDSG) erfasst. Zusätzlich dazu hat die Europäische Union supranational mit der Datenschutzgrundverordnung (DSGVO) einen europäischen Rahmen geschaffen, der von allen Mitgliedern eingehalten werden muss. In den wichtigsten Rechten entspricht die DSGVO dem BDSG, wobei die DSGVO im Zweifel den Vorrang gegenüber dem BDSG hat.

In den wichtigsten Rechten entsprechen sich DSGVO und BDSG jeweils. Demnach dürfen personenbezogene Daten nur für bestimmte, festgelegt Zwecke von Kunden erfasst und gespeichert werden. Außerdem hat ein Kunde, von dem personenbezogene Daten erhoben und gespeichert werden, jederzeit das Recht zu erfahren, welche Daten gespeichert werden und auch eine Verbesserung bei Fehlern oder Falschinformationen zu fordern. Kunden haben das Recht auf Einschränkung der Verarbeitung, wenn bestimmte Voraussetzungen erfüllt sind. Zudem haben Kunden auch das Recht die Löschung der personenbezogenen Daten zu fordern, wenn sie sehen, dass bestimmte Voraussetzungen der Datenspeicherung nicht mehr erfüllt sind.

Folgende wichtigste Rechte hat ein Kunde demnach im Zusammenhang mit der Erhebung, Speicherung und Weiterverarbeitung seiner personenbezogenen Daten:

Auskunftsrecht (Art. 15 DSGVO, § 34BDSG): Jeder – unabhängig von Alter, Wohnsitz und Nationalität – hat gegenüber nicht-öffentlichen Stellen nach § 34 Bundesdatenschutzgesetz (BDSG) das Recht auf Auskunft über die zu seiner Person gespeicherten Daten.[1]

Berichtigungsrecht (Art. 16 DSGVO, § 58 BDSG): Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen. [2]

[1]https://dsgvo-gesetz.de/art-15-dsgvo/, https://www.gesetze-im-internet.de/bdsg_2018/__34.html
2https://dsgvo-gesetz.de/art-16-dsgvo/, https://www.gesetze-im-internet.de/bdsg_2018/__58.html

Löschungsrecht (Art. 17 DSGVO, § 58 BDSG): Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

1. Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
2. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
3. Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2
   Widerspruch gegen die Verarbeitung ein.
4. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
5. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
6. Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben. [3]

Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO, § 58 BDSG): Die betroffene Person hat das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

1. die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
2. die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
3. der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
4. die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. [4]

[3]https://dsgvo-gesetz.de/art-17-dsgvo/,https://www.gesetze-im-internet.de/bdsg_2018/____58.html
[4]https://dsgvo-gesetz.de/art-18-dsgvo/, https://www.gesetze-im-internet.de/bdsg_2018/__58.html

12.2 Datensicherheit

Die Datensicherheit befasst sich mit dem generellen Schutz von sensiblen, meist personenbezogenen Daten innerhalb von Unternehmen. Zur Datensicherheit werden dabei Maßnahmen und Mechanismen gezählt, die das Ziel haben, ausschließlich berechtigten Personen Zugriff auf diese Daten zu gewähren und Unbefugte davon auszuschließen.

Folgende Anforderungen werden im Sinne der Datensicherheit an ein DBMS gestellt:

- Identifikation und Authentifizierung von Benutzern
- Autorisierung und Zugriffskontrolle
- Aufzeichnung von sicherheitsrelevanten Aktionen von Benutzern

Typische Schwachstellen der Systeme können dabei sein:

- Missbrauch von Autorität durch Diebstahl von Daten
- Maskierung von Code, da nicht autorisierte Benutzer zugreifen könnten (z. B. über eine SQL-Injection)
- Umgehen der Zugriffskontrolle durch Ausnutzung von Sicherheitslücken
- Durchstöbern von zugänglichen Dateien (z.B. Passwort-Dateien)
- Etc.

Möglichkeiten der Authentifizierung von Benutzern:

Interne Authentifizierung:

- Ein Benutzer wird in der Datenbank durch ein CREATE User Statement angelegt

- Passwort des Users wird in der Datenbank verschlüsselt abgespeichert

- Identifikation des Benutzers durch Kombination von Username und Passwort gewährt Zugriff auf die Datenbank und vorhandene Rechte können eindeutig zugeordnet werden

Externe Authentifizierung:

- Verifizierung der Identität durch externe Quellen (z.B. das Betriebssystem) durch ein

CREATE User externally Statement

- der Nutzer kann für mehrere DBs genutzt werden

Das Berechtigungskonzept

Das Berechtigungskonzept ist ein wichtiger Bestandteil bei der Planung, Verwaltung und Nutzung von Datenbanksystemen. Das Berechtigungskonzept regelt, welche Berechtigungen verteilt werden können und wie unbefugte Zugriffe auf das Datenbanksystem verhindert werden können. Dabei gilt der Grundsatz: nur als zwingend notwendig erachtete Berechtigungen werden den Benutzern des Datenbanksystems erteilt. Dadurch wird sichergestellt, dass nur zugriffsberechtigte Benutzer auch tatsächlich Zugriff erhalten.

Meist wird in der Praxis hierzu ein rollenbasiertes Berechtigungskonzept verwendet. Dabei werden Rechte zu verschiedenen Rollen zusammengefasst und Benutzer werden diesen Rollen zugeordnet. Damit soll sichergestellt sein, dass die Einfachheit der Rechtevergabe auf der einen Seite und die Sicherstellung von datenschutzrechtlichen Aspekten auf der anderen Seite gewährleistet werden.

Die Berechtigungsverwaltung hat die Aufgabe die Zugriffskontrolle auf Datenbank und vorhandene Datenobjekte zu gewährleisten. Das Datenbanksystem prüft dabei vor dem Zugriff das Vorhandensein von Rechten und die Gültigkeit entsprechender Berechtigungen.

Erstellung eines neuen Users und Vergabe eines Passworts:

```
CREATE USER username IDENTIFIED BY password ;
```

Vergabe von Rechten an einen bestehenden User:

```
GRANT privilege_name
ON object_name
TO {user_name |PUBLIC |role_name} [WITH GRANT OPTION]
FLUSH PRIVILEGES;
```

PRIVILEGE_NAME: dem User zugeteiltes Recht. Es werden zwei Arten von Privilegien unterschieden:
Systemprivilegien: gelten für das gesamte System: **CREATE, ALTER, DROP**.
Objektprivilegien: gelten nur für bestimmte Objekte der Datenbank: **SELECT, INSERT, UPDATE, EXECUTE, DELETE**.

EXECUTE erlaubt dabei die Ausführung einer Stored Procedure (Datenbankskript) oder einer Funktion.

OBJECT_NAME. Das Objekt; für das Rechte gewährt werden. Dies kann unter anderem eine Tabelle, Sicht, Prozedur etc. sein.

USER_NAME: Name des Users, für den Rechte gewährt werden.

PUBLIC: Rechte werden an alle User gewährt.

ROLLE_NAME: Name der Rolle. Rollen sind in diesem Zusammenhang eine Gruppe von zusammenhängenden Privilegien.

WITH GRANT OPTION: gewährt das Recht anderen Usern ebenfalls Rechte zu gewähren.

FLUSH PRIVILEGES: die Änderung an Berechtigungen wird erst durch Aktualisierung der Metadaten-Tabelle sichtbar, in der die Berechtigungen für alle User abgespeichert werden. In manchen Datenbankmanagementsystemen wird dieser Schritt automatisch ausgeführt.

Zum Beispiel:

```
GRANT SELECT ON tabellenname TO user
FLUSH PRIVILEGES ;

GRANT UPDATE ON tabellenname TO user
FLUSH PRIVILEGES ;

GRANT DELETE ON tabellenname TO user
FLUSH PRIVILEGES ;

GRANT ALL ON tabellenname TO user
FLUSH PRIVILEGES ;
```

Entziehen von Rechten von einem bestehenden User:

```
REVOKE privilege_name
ON object_name
FROM {user_name |PUBLIC |role_name}
FLUSH PRIVILEGES ;
```

Analog zu „GRANT“:

Zum Beispiel:

REVOKE SELECT ON tabellenname **FROM** user
FLUSH PRIVILEGES ;

REVOKE UPDATE ON tabellenname **FROM** user
FLUSH PRIVILEGES ;

REVOKE DELETE ON tabellenname **FROM** user
FLUSH PRIVILEGES ;

REVOKE ALL ON tabellenname **FROM** user
FLUSH PRIVILEGES ;

Metadaten für Berechtigungen

In relationalen Datenbankmanagementsystemen wie PostgreSQL sind Metadaten-Schemata definiert, die Metadaten speichern und die Datenbanken auf den jeweiligen Systemen verwalten. In PostgreSQL beispielsweise zwei Schemata implementiert, die Metadaten des Datenbankmanagementsystems beinhalten. Diese beiden Schemata sind auf der Oberfläche von pgAdmin nicht zu finden, so dass man diese explizit ansprechen muss.

Im Information_Schema und im PG_Catalog sind Daten innerhalb des Datenbankmanagementsystems gespeichert, die für die Selbstverwaltung des Systems unabdingbar sind. So können in diesen Metadaten-Tabellen systemseitige Tabellen gefunden werden, die wir uns für unser Datenbankmanagementsystem genauer anschauen werden.

Außerdem sind folgende weitere Mechanismen im Zusammenhang mit der Datensicherheit von Datenbanksystemen denkbar:

- Verschlüsselung der Kommunikation zwischen Client und Datenbankserver
- Protokollierung von Datenbankzugriffen in LOG-Dateien
- Nutzung einer privaten Datenbank