Dr. Daniel Quathamer
Zu den Birken 49
47269 Duisburg
Tel. 0203 / 41799186
Fax: 0203 / 41799187
danielq@memtext.de
www.memtext.de

Datenschutz in SuperX

LEITFADEN DATENSCHUTZ

http://www.superx-projekt.de

Datenschutz ist im Data Warehouse ein zentrales Thema. Dieses Dokument stellt zentrale Themen und Fragen zum Thema Datenschutz im Rahmen von kurzen Hinweisen und einer Linksammlung zu weiterführenden Informationen zusammen.

Version: 0.1
Stand: 26.09.2018

Inhaltsverzeichnis

1 Datenschutz

1.1 Einleitung

Bei Implementierung eines Data Warehouse stellen sich immer auch datenschutzrechtliche Fragen. Im Laufe der letzten Jahre und aufgrund der Zusammenarbeit mit der HIS e.G. den Hochschulen und Ministerien gibt das System von vornherein einige Antworten zu den Themen Datensparsamkeit, Transparenz, Datensicherheit und Performanz.

1.1.1 Datensparsamkeit

- Das System ist **modular** aufgebaut, die Hochschule kann einzelne Komponenten nutzen oder eben nicht. Wer z.B. die Studierendenverwaltung nutzt, aber keine Personalverwaltung, kann dies leicht durch Installation / Deinstallation von Komponenten tun.
- Das System liefert fertige **Schnittstellen** zu den HIS-Systemen bzw. konkrete Schnittstellenbeschreibungen für Nicht-HIS-Systeme. Es werden in der Regel nur die Tabellen entladen, die auch in den Berichten ausgewertet werden. Die Aufforderung zum Entladen kommt dabei von den Hopchschulen, d.h. der Bedarf steuert das System.
- Darüber hinaus wird i.d.R. der **Personenbezug** bei den Daten entfernt.
  - Bei Studierenden z.B. wird nicht der Personenname entladen, und die Matrikelnummer kann pseudonymisiert werden.
  - Bei der Finanz-Komponente können personenbezogene Daten wie Zahlungspartnernummer oder Verwendungszweck entfernt werden.
  - Eine Ausnahme ist die Personal Komponente, dort kann die Hochschule auch personenbezogene Daten laden, wenn diese in Berichten genutzt werden. Auch hier sind aber spezielle Pseudonymisierungs- und Anonymisierungsfunktionen enthalten.
- Bei Entfernung des Personenbezugs von Daten durch Pseudonymisierung und Anonymisierung findet dies bereits **beim Entladen** aus dem Vorsystem statt, d.h. die personenbezogenen Daten verlassen das Vorsystem nicht.
- Alle Datenbereiche lassen sich **zeitbezogen** entladen, z.B. Startjahr oder Startsemester. Bei der Personal-Komponente gibt es darüber hinaus spezielle Löschungskonzepte.

1.1.2 Datensicherheit

- Die Serverarchitektur bedingt, dass kein Anwender eine **direkte Datenbankverbindung** bekommt, d.h. die Gefahr von Missbrauch ist geringer als bei älteren Client-Server-Anwendungen.
- Das Vorsystem muss nicht unbedingt eine **Online-Verbindung** zum Data Warehouse bieten, die Daten können in festgelegten Rhythmen zum DWH kopiert werden.
- Nutzerverwaltung des Systems prüft bei jedem http-Zugriff die **Rechte** des angemeldeten Benutzers in Bezug auf Berichte, Institutionen innerhalb der Berichte, und Hierarchien innerhalb der Berichte. Siehe auch das Administrationshandbuch.
- Passworte werden **verschlüsselt** bzw. als Hash gespeichert.
- Die Abschottung des Data Warehouse obliegt der **IT-Abteilung**, es gibt konkrete Anleitungen zur Implementation des Systems. Darüber hinaus gibt es eine Checkliste für spezielle Sicherheitsmaßnahmen.

1.1.3 Transparenz

- Zunächst einmal ist es ein Vorteil, dass das System **standardisierte Schnittstellen** zum Vorsystem nutzt. Dies ist eine Vorbedingung für Transparenz. Sobald die Hochschule eigene Schnittstellen erstellt, muss sie die Transparenz mit aufwändigen Eigenmitteln herstellen. Aufwändigere Funktionen wie stichtagsbasiertes Entladen oder Pseudonymisierung sind nur schwer aus eigener Kraft zu implementieren.
- Generell ist der **Quellcode** der Schnittstellen offengelegt, d.h. jede Person mit SQL-Kenntnissen kann sich einen Überblick verschaffen.
- Da dieser Zugang für Nicht-Programmierer mühsam ist, gibt es darüber hinaus spezielle **Webseiten** zur Schnittstellendokumentation:
  - Dokumentation des **Entladescripts**, z.B. Personal-Komponente
  - Dokumentation des **Datenmodells** in SuperX, z.B. Personal-Komponente
  - Dokumentation der **Schnittstelle**, z.B. Personal-Komponente.
- Die Dokumentationen werden **automatisch** aus den Quellen erzeugt und sind daher immer aktuell.

1.1.4 Performanz und Verfügbarkeit

Das System muß eine hohe **Verfügbarkeit** bieten, d.h. Anwender müssen schnell Ergebnisse bekommen können.

- Daher laufen wichtige, aber zeitaufwändige Transformation scriptgesteuert in der **Nacht**. Beispielscripte liegen dafür vor, z.B. in der Personal-Komponente.
- Dazu gibt es u.a. die Möglichkeit des Lastausgleichs oder der Datenbank-Replikation. Dies sind allerdings keine Leistungsmerkmale des Systems, sondern von den zugrunde liegenden Technologien (Apache, Tomcat, DBMS). In dem System werden aber Beispielkonfigurationen mitgeliefert.
- Auch für Diensteinrichtung, Datenbankwartung und Server-Neustart werden **Beispielscripte** mitgeliefert.
- Das **Logging** ist transparent und kann speziell gesteuert werden.

1.2 Checkliste Sicherheitsmassnahmen

Um die Datensicherheit zu verbessern, empfehlen wir folgende Massnahmen:

1.2.1 SSL-Verschlüsselung mit Zertifikat von Trustcenter

Generell sollten Sie den Server immer mit SSL-Verschlüsselung betreiben, egal ob über Tomcat oder Apache.

Es wird an anderer Stelle beschrieben, wie Sie ein Zertifikat selbst erstellen können, dies sollte nur zu Testzwecken dienen. Lassen Sie stattdessen ein persönliches Zertifikat durch einen kommerziellen Zertifizierungsserver publizieren. Akkreditierte Anbieter von qualifizierten Zertifikaten gemäß Deutschem Signaturgesetz sind die AuthentiDate International AG, verschiedene Bundesnotarkammern, D-TRUST (Bundesdruckerei-Gruppe), DATEV, Deutsche Post, TC Trustcenter, T-Systems und S-Trust Sparkassen-Finanzgruppe.

1.2.2 Einstellungen zur Passwortsicherheit

Bitte folgen Sie den Empfehlungen von Zendas zur Passwortsicherheit. Die Zentrale Datenschutzstelle der baden-württembergischen Universitäten macht folgende Empfehlung:

Passwortgültigkeit (Tage)	90-180
Passwort Groß- u. Kleinb.	1
Passwort erfordert Ziffer	1
Passwortlänge (Minimum)	8

Diese Einstellungen können in der Konstanten-Tabelle geändert werden.

Der Administrator kann erzwingen, dass der Benutzer sein Passwort ändern muss, indem er im XML-Frontend den entsprechenden User bearbeitet und bei "User muss Passwort ändern" ein Häkchen setzt.

1.2.3 Servertrennung für maximale Sicherheit

Für maximale Sicherheit empfiehlt es sich physikalisch getrennte Server für Apache, Tomcat und die Datenbank zu betreiben. Des Weiteren sollten die Server durch eine Firewall abgeschottet werden, normalerweise steht der Apache-Server in der DMZ.

1.2.4 Keine Anzeige von internen Details bei Fehlermeldungen

Schalten Sie den Entwicklungsmodus aus, damit keine detaillierten Fehlermeldungen bei SQL-Abfragen nach außen angezeigt werden.

Setzen Sie in `$WEBAPP/WEB-INF/db.properties` „developmentMode“ auf „false“.

Eine weitere Verschleierungstechnik stellt das Aktivieren einer eigenen allgemeinen Fehlermeldung dar. Dadurch soll verhindert werden, das weitere Details – wie zum Beispiel der Java-Stacktrace – angezeigt wird. Richten Sie dafür eine Html-Datei `error.htm` ein, in der könnte zum Beispiel stehen:

```
"Es ist ein Fehler aufgetreten. Bitte wenden Sie sich an admin@universitaet.de"
```

Editieren Sie anschließend `$WEBAPP/WEB-INF/web.xml` und fügen an das Ende der Datei (also vor dem Endtag </web-app>) folgenden Abschnitt ein:

```
<error-page>
<error-code>500</error-code>
<location>/error.htm</location>
</error-page>
```

1.2.5 Sperren der DBFORMS-Komponente

Die DBFORMS-Komponente des XML-Frontends dient nur der Datenbankadministration und kann daher in Produktivsystemen mit WWW-Anbindung deaktiviert werden. Damit sind von außen

keine Datenbankverbindungen mehr möglich.
Eine Abschaltung der DBFORMS beeinträchtigt in keiner Weise die "normalen" Funktionen zur Berichtserstellung. Wenn die DBFORMS-Komponente benötigt wird, kann eine Installation der betreffenden Module in einem separaten Tomcat auf einem lokalen oder besonders geschützten System stattfinden, wo die DBFORMS dann freigeschaltet werden können.

1.2.6 Logging von Aktivitäten im Adminbereich (dbforms)

Das Logging für DBFORMS wird in der Datei `$WEBAPP/WEB-INF/log4j.properties` festgelegt. Passen Sie die Datei entsprechend Ihrer Erfordernisse an.

1.2.7 Kontrolle des Referers

Zur Steigerung der Sicherheit kann eingestellt werden, dass bei aufgerufenen Links kontrolliert wird, ob auch ein bestimmter Referer im Request-Parameter enthalten ist.

Um diese Funktion zu aktivieren, fügen Sie den folgenden Abschnitt als zusätzlichen Parameter zum SuperXManager-Servlet in der `$WEBAPP/WEB-INF/web.xml` hinzu:

```
<init-param>
<param-name>referer_start</param-name>
<param-value>https://webserver/superx</param-value>
</init-param>
```

Es ist allerdings zu berücksichtigen, dass einige Browser erlauben, die Übermittlung des Referrers zu deaktivieren. Auch Content-Filter (sowohl im Browser als auch auf Proxys) können entsprechend eingestellt werden. Ein Aufruf mittels IP-Nummer statt Rechnername würde ebenfalls dann fehlschlagen.

1.2.8 Directory-Listing in Tomcat/Apache abschalten

Kontrollieren Sie, dass die Funktion Directory-Listing sowohl im Apache als auch im Tomcat abgeschaltet ist.

In Tomcat muss in der Datei $TOMCAT_HOME`/conf/web.xml` im folgenden Abschnitt der Eintrag für listings auf false gesetzt werden.

```
<servlet>
        <servlet-name>default</servlet-name>
                <servlet-class>org.apache.catalina.servlets.DefaultServ-
let</servlet-class>
            <init-param>
                <param-name>debug</param-name>
                <param-value>0</param-value>
            </init-param>
            <init-param>
                <param-name>listings</param-name>
                <param-value>false</param-value>
            </init-param>
```

```
        <load-on-startup>1</load-on-startup>
</servlet>
```

1.2.9 Kontrolle von (fehlerhaften) Anmeldungen

Kontrollieren Sie die Tabelle `protokoll` auf Häufung von Fehlanmeldungen (`proto_fkt_id=2`), z.B. per cron-job.

Wenn Sie zusätzlich erfolgreiche Anmeldungen loggen wollen, setzen Sie den Eintrag "`Erweitertes Protokoll`" in der konstanten-Tabelle auf `apnr=1` und starten Sie Tomcat neu.