



datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, CH-8090 Zürich

Tel.: 043 259 39 99
Fax: 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch

Einführung und Übersicht (inklusive Installation und Anpassung GS-Tool)

Informationssicherheit in Gemeinden Bevölkerungszahl > 4000



**Datenschutz
mit Qualität**

Inhalt

1. Ausgangslage	3
2. Dokumente und Hilfsmittel	4
2.1 Übersicht	4
2.2 Hilfsmittel	5
2.2.1 Massnahmenkataloge	5
2.2.2 GS-Tool BSI, Modell GS-Tool Gemeinde	5
3. Umsetzung der Anforderungen an die Informationssicherheit	6
3.1 Schritt 1: Festlegen der Sicherheitsstrategie	6
3.2 Schritt 2: Aufbau der Organisationsstruktur für Informations- sicherheit	6
3.3 Schritt 3: Erstellen des IKT-Sicherheitskonzepts	7
3.3.1 Inventar der Systeme und Anwendungen	7
3.3.2 Verknüpfen der neuen Objekte	7
3.3.3 Klassifizieren der Systeme und Anwendungen	8
3.3.4 Zuweisen der Sicherheitsmassnahmen	9
3.3.5 Soll-Ist-Vergleich der Massnahmen	9
3.3.6 Realisierungsplanung	10
3.4 Schritt 4: Umsetzen der Sicherheitsmassnahmen	10
3.4.1 Erstellen der Weisungen für die Mitarbeitenden	10
3.4.2 Planen der Sensibilisierung der Mitarbeitenden	11
3.4.3 Erstellen eines Rollen- und Berechtigungskonzepts	11
4. Halten des Informationssicherheitsniveaus	12
4.1 Allgemeines	12
4.1.2 Regelmässige Überprüfung der Umsetzung der Massnahmen	12
4.1.3 Regelmässige Überprüfung und Anpassung der Massnahmen	12
5. Installation und Update GS-Tool	13
5.1 Installation	13
5.2 Update (Metadaten-Update)	14
6. Links	15

1. Ausgangslage

Anlässlich der vom Datenschutzbeauftragten (DSB) durchgeführten Kontrollen hat sich gezeigt, dass in vielen Gemeinden dieselben Mängel im Bereich Informationssicherheit bestehen. Einerseits fehlen Grundlagendokumente wie beispielsweise die Leitlinie zur Informationssicherheit, andererseits werden Massnahmen im organisatorischen und technischen Bereich wie etwa die Regelung und Umsetzung des Passwortgebrauchs nicht oder nur mangelhaft umgesetzt.

Der DSB stellt im Folgenden Anleitungen, Vorlagen, Beispiele und Instrumente zur Verfügung. Diese erleichtern die Umsetzung der Anforderungen des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) an die Informationssicherheit. Je nach Art der Vorlage wurden diese an die Bedürfnisse respektive an die Grösse der Gemeinde in Bezug auf die Bevölkerungszahl angepasst.

Dieses Dokument richtet sich an Gemeinden mit mehr als 4000 Einwohnerinnen und Einwohnern.

2. Dokumente und Hilfsmittel

2.1 Übersicht

Art	Thema
Einführung und Übersicht	Informationssicherheit in Gemeinden (inklusive Installation und Anpassung GS-Tool)
Glossar und Abkürzungsverzeichnis	Glossar und Abkürzungen Informationssicherheit
Anleitungen	Aufbau Organisationsstruktur Informationssicherheit
	Sensibilisierung der Mitarbeitenden für Informationssicherheit
Vorlagen	Leitlinie zur Informationssicherheit
	Weisung zur Informationssicherheit
	Erklärung zur Informationssicherheit
Beispiel	Rollen- und Berechtigungskonzept Gemeinde X
Checklisten	Minimummassnahmenkatalog
	Inhaltsverzeichnis Betriebsdokumentation

Es stehen eine Einführung in das Thema, Anleitungen, direkt anwendbare Vorlagen, Beispiele und Checklisten zur Verfügung.

Das vorliegende Dokument „Einführung und Übersicht – Informationssicherheit in Gemeinden“ gibt den Gemeinden, respektive deren Mitarbeitenden, eine Übersicht über die vom Gesetz über die Information und den Datenschutz (IDG, LS 170.4) geforderten Massnahmen sowie eine Einführung, wie diese mit welchen Mitteln umgesetzt werden können.

Die Anleitungen enthalten konkrete Hinweise, wie:

- eine geeignete Struktur für die Umsetzung der Informationssicherheit geschaffen werden kann
- die Mitarbeitenden laufend mit Blick auf diese Thematik sensibilisiert werden können

Die Vorlagen können nach Vornahme der auf die Gemeinde abgestimmten Anpassungen (Dokumentenvorlage der jeweiligen Gemeinde, Gemeindennamen, Namen der verantwortlichen Behörden, Auswahl der Formulierungsvarianten, Erlass durch das zuständige Organ usw.) direkt eingesetzt werden.

Das Beispiel Rollen- und Berechtigungskonzept Gemeinde X bedarf zur Übernahme einer umfassenden Anpassung an die Gemeindeverhältnisse.

2.2 Hilfsmittel

Zur Verfügung stehen folgende Mittel, respektive Instrumente:

- Massnahmenkatalog N1 / N2
- GS-Tool Gemeinde (Massnahmenkatalog N2 ist integriert)

2.2.1 Massnahmenkataloge

Die Massnahmenkataloge beinhalten die vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) geforderten wichtigsten umzusetzenden Massnahmen, um die Informationssicherheit zu gewährleisten.

Der DSB hat die über 1000 Massnahmen des BSI-Grundschutzkatalogs nach den Bedürfnissen der Gemeinden, abgestuft nach deren Einwohnerzahl, angepasst:

Katalog	Bevölkerungszahl Gemeinde	Anzahl Massnahmen
Massnahmenkatalog N1	< 4000	ca. 130 Massnahmen
Massnahmenkatalog N2	> 4000	ca. 400 Massnahmen

2.2.2 GS-Tool BSI, Modell GS-Tool Gemeinde

Das BSI stellt die Software GS-Tool BSI zur Verfügung, welche das Planen, Umsetzen, Überprüfen und Weiterentwickeln der Sicherheitsmassnahmen des IKT-Sicherheitskonzepts wesentlich erleichtert. Diese Software, welche beim BSI heruntergeladen werden kann, wurde, ebenso wie die Massnahmenkataloge, auf die Bedürfnisse der mittleren und grösseren Gemeinden, also auf diejenigen mit einer Bevölkerungszahl von mehr als 4000, angepasst (GS-Tool Gemeinde). Zur Implementierung und Anpassung dieser Software siehe unter Ziff. 5 dieses Dokuments.

Vor Beginn der Verwendung des GS-Tools Gemeinde empfiehlt es sich, folgenden Online-Kurs zu absolvieren:

https://www.bsi.bund.de/ContentBSI/gstool/wbtgstool/index_hm.html

Das GS-Tool Gemeinde weist folgende Vorzüge auf:

- Vielzahl von Anleitungen / Erfahrungen
- Breiter Funktionsumfang
- Vordefinierte Berichte
- Einfügen individueller Bausteine (Massnahmen) möglich
- Ausführliche Beschreibung der Massnahmen inkl. der Rollenverknüpfung
- Gute Darstellung und Verwaltung von Beziehungen
- Gute Support- und Update-Leistungen

Für kleinere Gemeinden, also solche mit einer Bevölkerungszahl unter 4000, genügt ein schriftliches IKT-Sicherheitskonzept, welches mit einer Standardsoftware wie Microsoft Office gepflegt werden kann.

3. Umsetzung der Anforderungen an die Informationssicherheit

Die Umsetzung der Anforderungen an die Informationssicherheit in den Gemeinden erfolgt grundsätzlich in vier Schritten:

1. Festlegen der Sicherheitsstrategie
2. Aufbau der Organisationsstruktur für Informationssicherheit und Verteilung der Rollen und Verantwortungen
3. Erstellen des IKT-Sicherheitskonzepts mit dem GS-Tool
 - Inventar der Systeme und Anwendungen
 - Verknüpfen der neuen Objekte
 - Klassifizieren der Systeme und Anwendungen
 - Zuweisen der Sicherheitsmassnahmen
 - Soll-Ist-Vergleich der Sicherheitsmassnahmen
 - Realisierungsplanung
4. Umsetzen der fehlenden Sicherheitsmassnahmen

3.1 Schritt 1: Festlegen der Sicherheitsstrategie

Die Sicherheitsstrategie wird in einer Leitlinie zur Informationssicherheit dokumentiert. Das angestrebte Sicherheitsniveau wird festgehalten und die Sicherheitsziele werden allen Mitarbeitenden zugänglich gemacht.

Die Sicherheitsziele sind grundsätzlich bei allen Gemeinden dieselben, weshalb der DSB eine Vorlage Leitlinie zur Informationssicherheit zur Verfügung stellt.

Was ist zu tun

1. Layout ans Corporate Design anpassen
2. Inhalt überprüfen und anpassen
3. Inkraftsetzung durch einen Beschluss der Exekutive (Gemeinderat)
4. Leitlinie an einem für alle Mitarbeitenden gut zugänglichen Ort publizieren

3.2 Schritt 2: Aufbau der Organisationsstruktur für Informationssicherheit

Um das von einer Gemeinde angestrebte Informationssicherheitsniveau zu erreichen, muss der Informationssicherheitsprozess gemeindeweit umgesetzt werden. Es muss eine Organisationsstruktur aufgebaut, die Rollen festlegt und diesen die Aufgaben zugeordnet werden. Der DSB stellt eine Anleitung für den **Aufbau der Organisationsstruktur für Informationssicherheit in Gemeinden** zur Verfügung.

Was ist zu tun

1. Rollenträgerinnen und -träger definieren
2. Aufgaben in die Stellenbeschreibungen integrieren
3. Notwendige Ressourcen den Mitarbeitenden zuweisen
4. Ausbildungsmassnahmen durchführen

3.3 Schritt 3: Erstellen des IKT-Sicherheitskonzepts

Das Erstellen des Sicherheitskonzepts kann unter Verwendung des GS-Tools Gemeinde erfolgen. Eine Anleitung zum Erstellen von IKT-Sicherheitskonzepten und zur Verwendung des GS-Tools ist veröffentlicht unter:

<https://www.bsi.bund.de/ContentBSI/gstool/download/handbuch/handbuch.html>

Das Vorgehen bei der Installation des GS-Tool Gemeinde wird in Ziff. 5.1 erläutert.

3.3.1 Inventar der Systeme und Anwendungen

Bei diesem Inventar handelt es sich um das Erfassen der Stammdaten. Damit ein bedrohtes Objekt geschützt werden kann, muss seine Existenz bekannt sein. Für die Informationssicherheit ist ein qualitativ hochwertiges Inventar unerlässlich.

Da sich das Inventar vielmals ändert und dies – aufgrund der Vernetzung – Einfluss auf die Sicherheit anderer bedrohten Objekte hat, ist es sinnvoll diese Abhängigkeiten in einer Software abzubilden.

Der DSB hat das GS-Tool BSI auf die Bedürfnisse der Gemeinden abgestimmt und stellt das GS-Tool Gemeinde zur Verfügung, in welcher die wichtigsten Räume, Anwendungen und Systeme bereits eingetragen sind.

Was ist zu tun

Das gruppierte Inventar ist an die Gemeindestruktur anzupassen (Applikationen, Server, Clients, Räume, Mitarbeitende usw. sind zu erfassen).

Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/03_StammdatenErfassen/stammdatenerfassen_node.html

3.3.2 Verknüpfen der neuen Objekte

Beim Verknüpfen handelt es sich um das Strukturieren der Stammdaten. Wurden weitere IKT-Objekte ins Modell eingefügt, müssen diese per Drag&Drop verknüpft werden (in der "Struktur-Ansicht").

Was ist zu tun

1. Neue Mitarbeitende auf die Anwendungen "ziehen", mit der sie arbeiten.
2. Neue Anwendungen auf die Systeme "ziehen", von denen sie abhängig sind.
3. Neue Systeme auf die Räume "ziehen", in denen sie sich befinden.
4. Neue Räume auf die Gebäude "ziehen", in denen sie sich befinden.

Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/04_StammdatenStrukturieren/stammdatenstrukturieren_node.html

3.3.3 Klassifizieren der Systeme und Anwendungen

Beim Klassifizieren handelt es sich um die Risikobeurteilung nach der Informatiksicherheitsverordnung (ISV). Damit die bedrohten Objekte angemessen geschützt werden können, muss der Schutzbedarf gemäss den Schutzzielen der ISV festgelegt sein.

Der DSB hat die bedrohten Objekte in seinem Modell bereits klassifiziert.

Was ist zu tun

1. Die Klassifizierung ist zu überprüfen bzw. zu erstellen

The screenshot shows the GSTOOL47 interface with a tree view on the left and a detailed view on the right. The tree view includes categories like 'Anwendung', 'Fachaufgabe', 'Schutzbedarf', and 'Ergänzende Sicherheitsanalyse'. The 'Finanzbuchhaltung' application is selected. The detailed view shows the following classification:

Grundwert	Schutzbedarf	Begründung
Vertraulichkeit:	normal	keine besonderen Personendaten
Vorschlag:	[(keine Angabe)]	
Integrität:	hoch	Vorgabe für Auszahlungen
Vorschlag:	[(keine Angabe)]	
Verfügbarkeit:	normal	Ausfall verkräftbar
Vorschlag:	[(keine Angabe)]	

Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/05_SchutzbedarfDokumentieren/schutzbedarfdokumentieren_node.html

2. Die Schutzbedarfskategorien sind allenfalls anzupassen

Siehe unter IT-Grundschutz benutzerdefiniert => Register: Schutzbedarfsdefinitionen

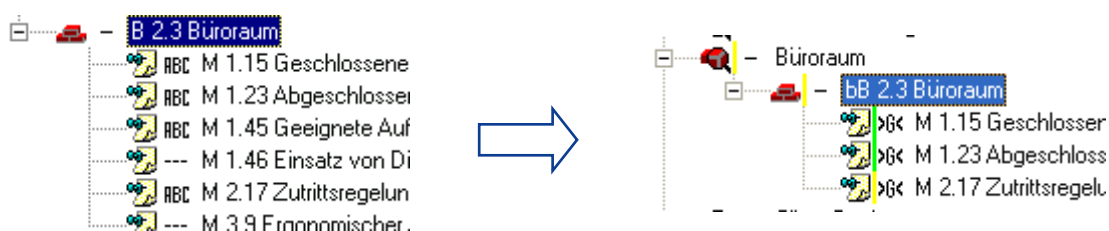
3.3.4 Zuweisen der Sicherheitsmassnahmen

Beim Zuweisen der Sicherheitsmassnahmen handelt es sich um die Modellierung. Das GS-Tool Gemeinden weist beim Erfassen neuer IT-Objekte automatisch einen (passenden) BSI-Baustein zu. Dieser enthält aber die vollständigen BSI-Massnahmen und nicht den reduzierten Katalog des DSB.

Was ist zu tun

Um mit dem reduzierten Katalog arbeiten zu können, müssen die BSI-Bausteine durch individuelle Bausteine ersetzt werden. Diese sind speziell nummeriert (bB X.XX).

Beispiel:



Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/06_ITGrundschutzPruefen/03_VerknuepfungenErgaenzen/verknuepfungenergaenzen_node.html

3.3.5 Soll-Ist-Vergleich der Massnahmen

Beim Basis-Sicherheitscheck wird gemäss IT-Grundschutz des BSI überprüft, ob die nach IT-Grundschutz empfohlenen Massnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden Sicherheitsmassnahmen noch fehlen.

Was ist zu tun

Umsetzungsgrad jeder Massnahme (ja, teilweise, nein, entbehrlich) eintragen.

Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/06_ITGrundschutzPruefen/05_BSC1/bsc1_node.html

3.3.6 Realisierungsplanung

Ist der Umsetzungsgrad der erforderlichen Massnahmen bekannt, folgt die Realisierungsplanung.

Was ist zu tun

1. Will man die Sicherheitskosten berechnen, sind für jede Massnahme die Kosten einzutragen.
2. Die Verantwortlichkeiten (wer macht was?) sind bei jeder Massnahme einzutragen, bzw. die Vorschläge zu überprüfen.

Anleitung

https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursGSTOOL47/02_Anwendung/06_ITGrundschutzPruefen/09_Realisierung1/realisierung1_node.html

3.4 Schritt 4: Umsetzen der Sicherheitsmassnahmen

Bei der Umsetzung sind folgende zentrale Massnahmen prioritär zu behandeln.

3.4.1 Erstellen der Weisungen für die Mitarbeitenden

Der DSB stellt die Vorlage Weisung zur Informationssicherheit zur Verfügung.

Was ist zu tun

1. Layout ans Corporate Design anpassen
2. Inhalt überprüfen und bei Bedarf anpassen oder Variante auswählen
3. Inkraftsetzung durch das zuständige Organ (z.B. Gemeinderat)
4. Abgabe an die Mitarbeitenden, allenfalls mit Unterschrift bestätigen lassen
(Vorlage Erklärung zur Informationssicherheit)
5. Publikation an einem für alle Mitarbeitenden gut zugänglichen Ort

3.4.2 Planen der Sensibilisierung der Mitarbeitenden

Sensibilisierungsmassnahmen sind zu planen und umzusetzen.

Siehe Anleitung **Sensibilisierung der Mitarbeitenden für Informationssicherheit**

Was ist zu tun

1. Bedürfnisse der Gemeinde abklären
2. Planung und Umsetzung anhand der Anleitung vornehmen

Anleitung BSI (B 1.13):

<https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b01/b01013.html>

3.4.3 Erstellen eines Rollen- und Berechtigungskonzepts

Siehe Beispiel **Rollen- und Berechtigungskonzept der Gemeinde X**

Was ist zu tun

1. Beispiel des Rollen- und Berechtigungskonzept umfassend an die Bedürfnisse der Gemeinde anpassen

Anleitungen BSI (M 2.30, M 2.31):

<https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02030.html>

<https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02031.html>

4. Halten des Informationssicherheitsniveaus

4.1 Allgemeines

Das angestrebte Sicherheitsniveau ist dauerhaft zu gewährleisten, weshalb die Massnahmen regelmässig überprüft und fortlaufend verbessert werden müssen.

Dies betrifft sowohl die Umsetzung selbst als auch die Umsetzbarkeit des IKT-Sicherheitskonzepts und bedeutet:

1. Kontrollieren, inwieweit Sicherheitsmassnahmen in den einzelnen Bereichen umgesetzt wurden (Revision der Informationssicherheit): siehe Ziff. 4.1.2.
2. Prüfen, ob bestimmte Massnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), siehe Ziff. 4.1.3.

Ziel dieser Überprüfungen ist es, Mängel zu beheben. Die Akzeptanz dieser Überprüfungen wird erhöht, wenn dies den Mitarbeitenden kommuniziert wird.

4.1.2 Regelmässige Überprüfung der Umsetzung der Massnahmen

Die im IKT-Sicherheitskonzept geplanten Massnahmen müssen gemäss Realisierungsplan umgesetzt werden. Der Stand der Umsetzung muss dokumentiert werden. Termine und Ressourcen müssen überwacht und gesteuert werden. Die Leitungsebene (Gemeindeschreibende) ist regelmässig zu informieren.

4.1.3 Regelmässige Überprüfung und Anpassung der Massnahmen

Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden Sicherheitsmassnahmen.

Deshalb sollten diese mindestens einmal jährlich an im Voraus bestimmten Terminen überprüft werden und auch immer dann, wenn

- neue Geschäftsprozesse, Anwendungen oder IT-Komponenten aufgebaut werden
- grössere Änderungen der Infrastruktur vorgenommen werden (z. B. Umzug)
- grössere organisatorischen Änderungen anstehen (z. B. Outsourcing)
- sich die Gefährdungslage wesentlich ändert
- gravierende Schwachstellen oder Schadensfälle bekannt werden

Weiter sind auch unangekündigte Überprüfungen der Massnahmen sinnvoll.

Die in den einzelnen Überprüfungen ermittelten Ergebnisse sind zu dokumentieren. Es ist festzulegen, wie mit den Überprüfungsergebnissen zu verfahren ist.

Detaillierte Beschreibung vom BSI:

<https://www.bsi.bund.de/ContentBSI/grundschatz/kataloge/m/m02/m02199.html>

5. Installation und Update GS-Tool

5.1 Installation

1. Download der aktuellen Version

https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/Download/download_node.html

2. Installation des GS-Tool BSI gemäss folgender Anleitung

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/GSTOOL/gstool45_inst_pdf.pdf?__blob=publicationFile

Vier Schritte:

- Entpacken aller Dateien in ein Verzeichnis auf Ihrer Festplatte und starten des Programms "setup.exe"
- Löschen des Verzeichnisses nach abgeschlossener Installation
- Zu beachten: zur Installation der Software werden Administratorrechte auf Ihrem PC benötigt
- Im Anschluss an die Installation der Anwendung unbedingt das Servicepack 2 für GS-Tool 4.5 installieren

Das Servicepack finden Sie auf der Seite GS-Tool-Servicepacks (https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/Download/ServicepacksfuerGSTOOL/servicepacksfuergstool_node.html). Durch Installation dieses Servicepacks erhält das GS-Tool die Versionsnummer 4.7

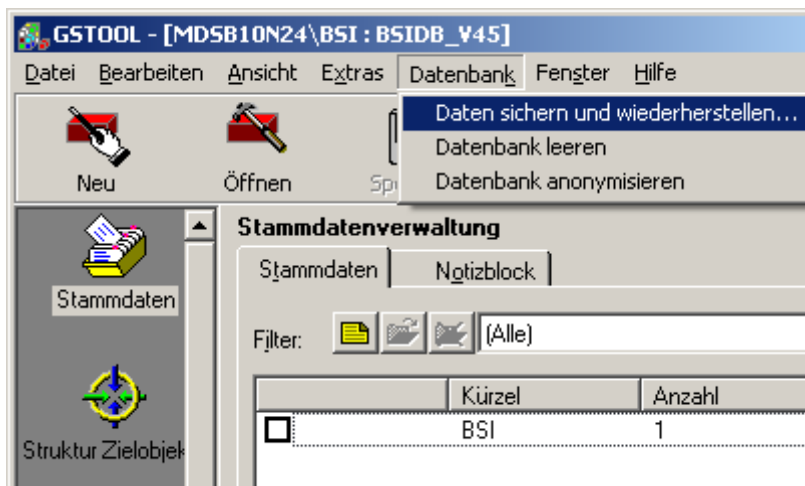
3. Download der Datenbank für das GS-Tool

https://review.datenschutz.ch/BSIDB_V47_Modell_Gemeinden_23122011.zip

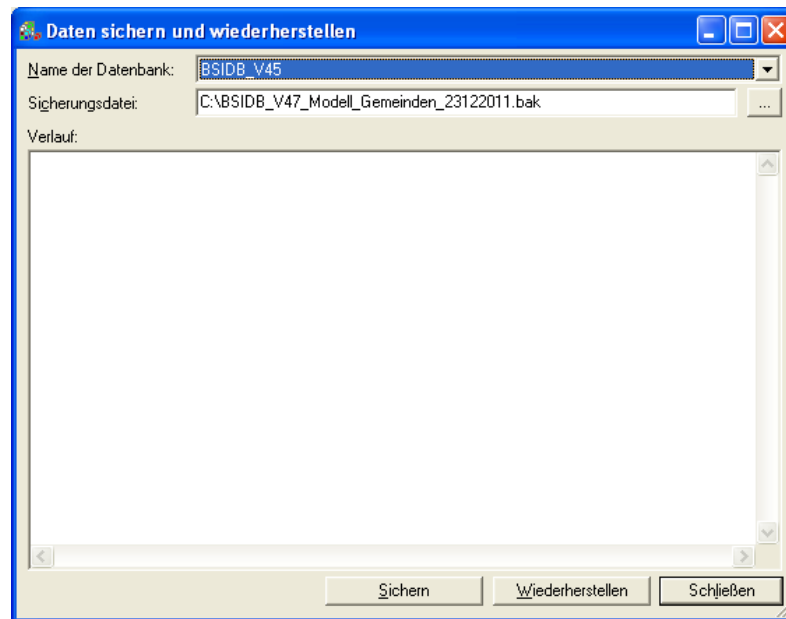
4. Entpacken Zip-Archiv

(z.B. in "C:\BSIDB_V47_Modell_Gemeinden_23122011.bak")

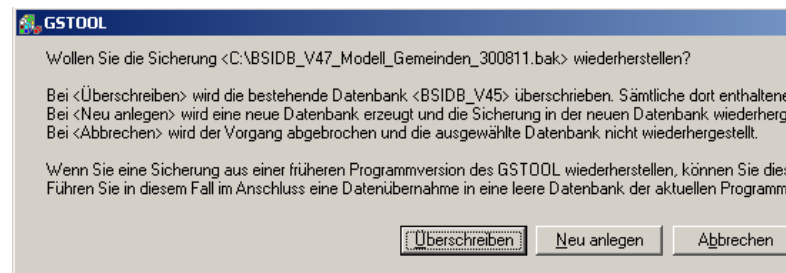
5. Import der Datenbank ins GS-Tool BSI



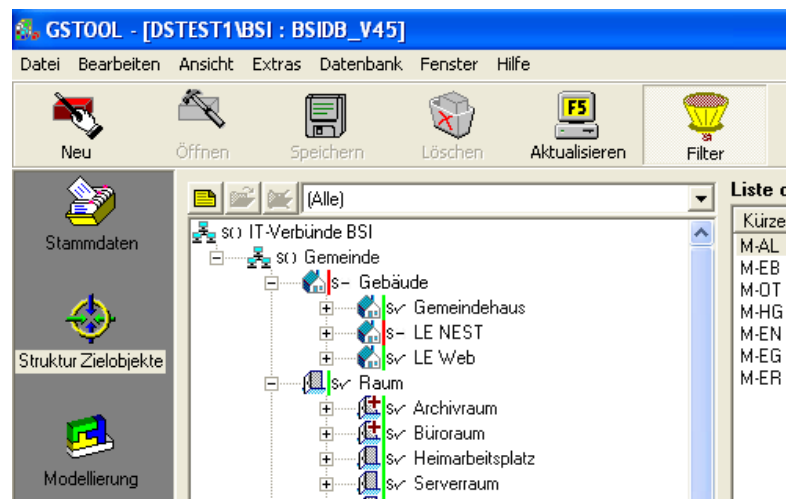
"Datenbank" ->
"Daten sichern
und wiederher-
stellen..."



1. ".bak"-Datei auswählen (...)
2. "Wiederherstellen" klicken



Auf "Überschreiben" klicken



Nach einem Neustart sollte diese Struktur vorhanden sein

5.2 Update (Metadaten-Update)

Folgt bei dem ersten Update (12. Ergänzungslieferung BSI) -> Anfangs 2012

6. Links

Link	Inhalt
https://www.bsi-fuer-buerger.de/	Sicherheitsthemen benutzerfreundlich erklärt
https://www.bsi.bund.de/grundschutz	Umfangreiche Anleitung für das Erstellen eines IKT-Sicherheitskonzepts nach IT-Grundschutz. Detaillierte Massnahmenbeschreibungen.
https://www.bsi.bund.de/gstool	Webseite des BSI-Grundschutztools (GS-Tool)-> Downloads, Schulungen, Benutzerhandbuch usw.
http://www.datenschutz.ch	Diverse Vorlagen und Anleitungen betreffend Datenschutz und Informationssicherheit.
https://review.datenschutz.ch/	Online-Anwendung, um seine Informatik zu überprüfen.
https://passwortcheck.datenschutz.ch/	Anwendung, um die Sicherheit seines Passwortes zu überprüfen.