

Grundschutztools

23.02.2003

RRZE

Volkmar Scharf

Volkmar.Scharf@rrze.uni-erlangen.de

- **Kurzüberblick Vorgehensmodell BSI**
- **Grundschutztools im Überblick**
 - **GST BSI v. 3.0**
 - **GST Fa. Seconet**
- **Einsatzszenarien von Grundschutztools**
- **Diskussion**

- **Das BSI beschreibt im Grundschatzhandbuch standardisierte Vorgehensweisen**

IT-Sicherheitsprozeß nach BSI

V. Scharf, 23.01.2003

Überblick



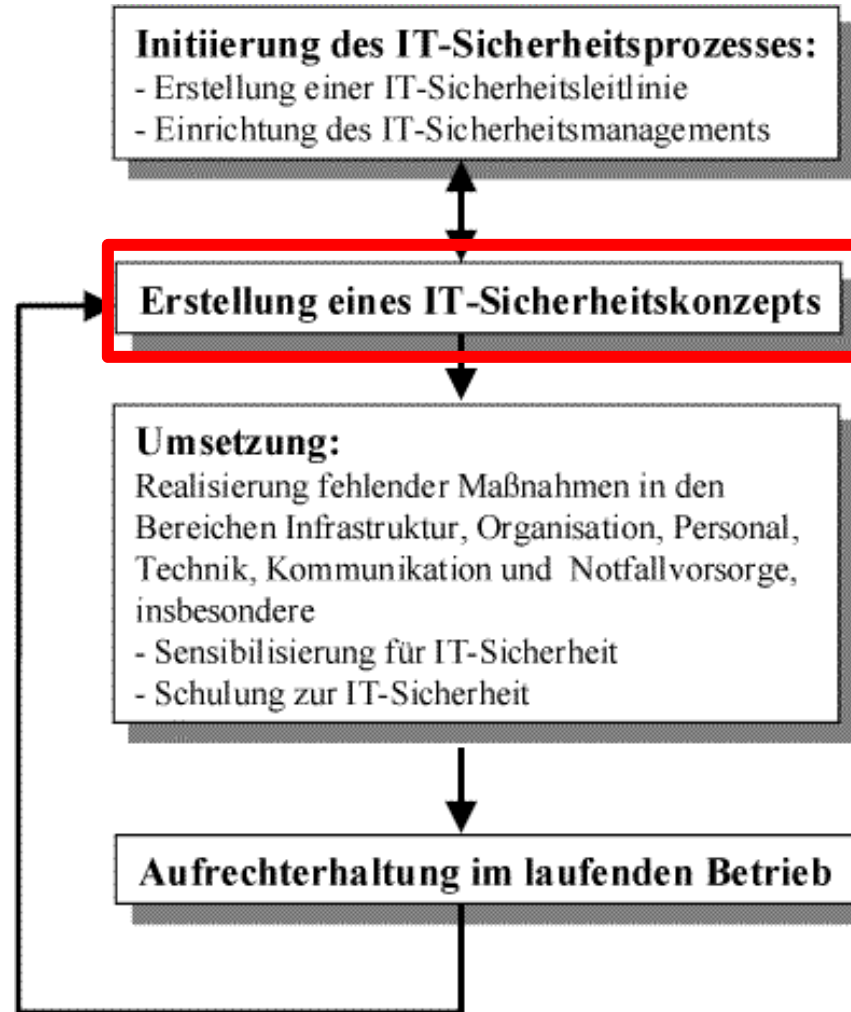
Quelle:
BSI

RRZE

IT-Sicherheitsprozeß nach BSI

V. Scharf, 23.01.2003

Überblick



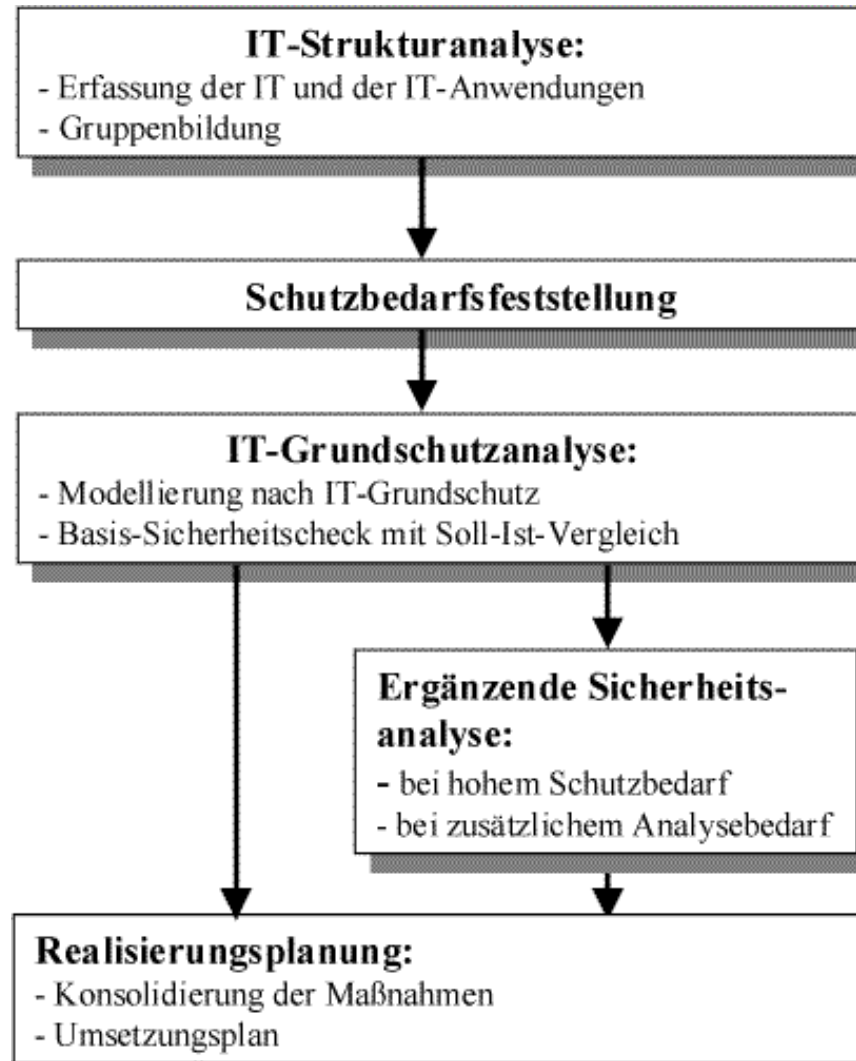
Quelle:
BSI

RRZE

IT-Sicherheitskonzept nach BSI

V. Scharf, 23.01.2003

Überblick



Quelle:
BSI

RRZE

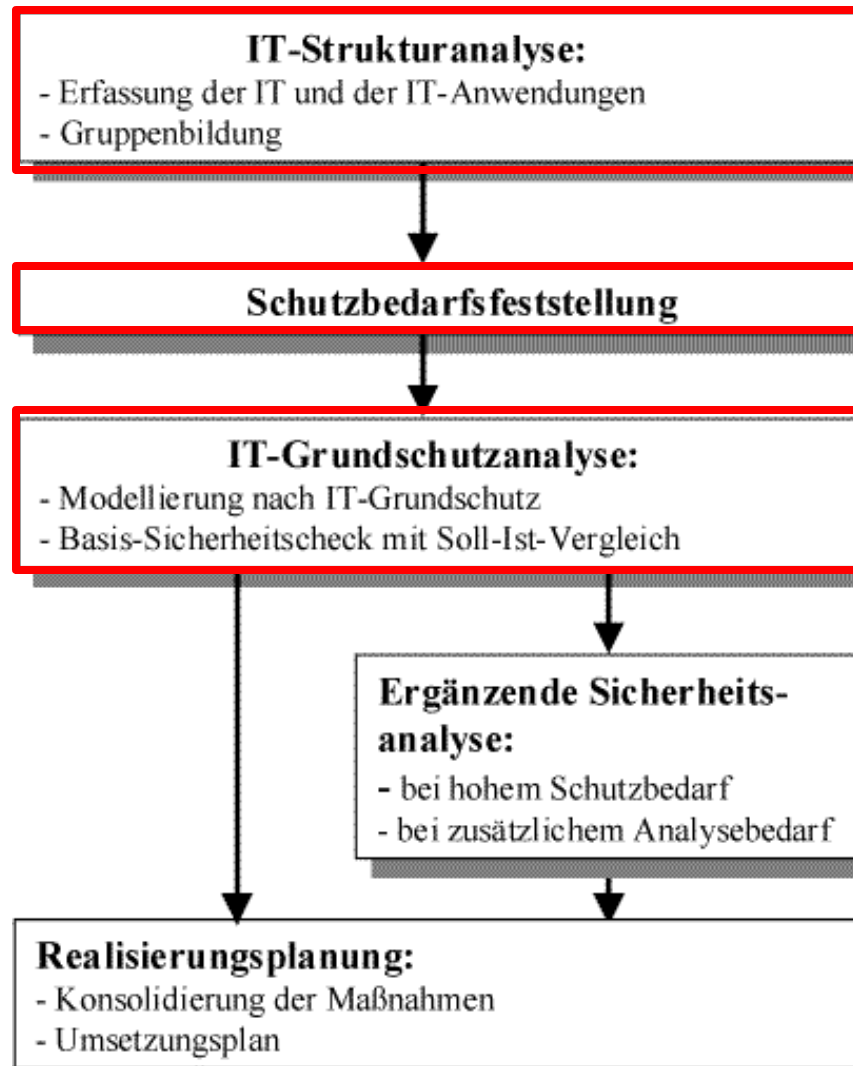
IT-Sicherheitskonzept nach BSI

V. Scharf, 23.01.2003

Überblick

Vom Tool
unterstützt

Quelle:
BSI



Grundschatztools

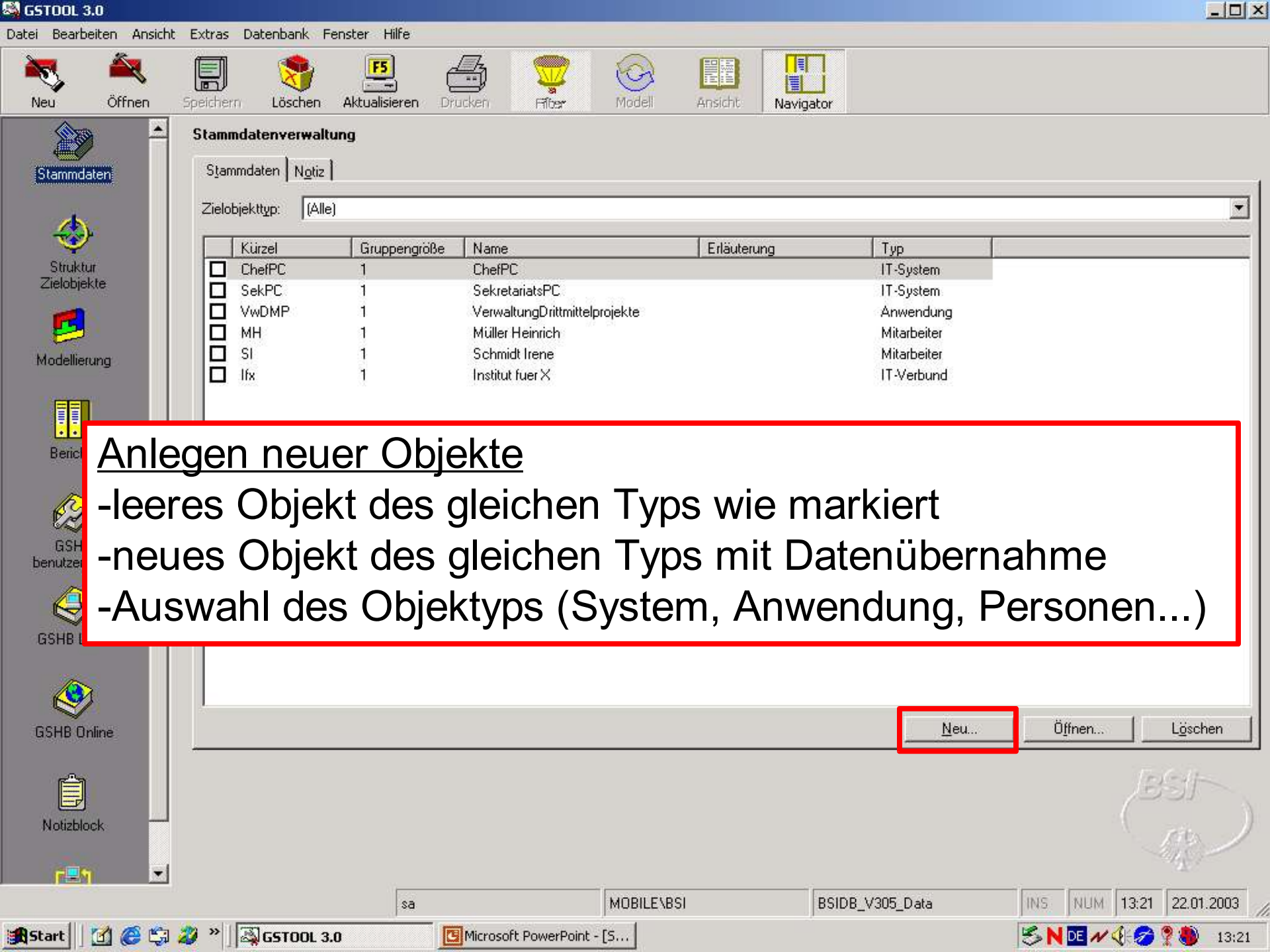
RRZE

Quelle: <http://www.bsi.de/gstool/index.htm>

30 Tage Demo kostenfrei

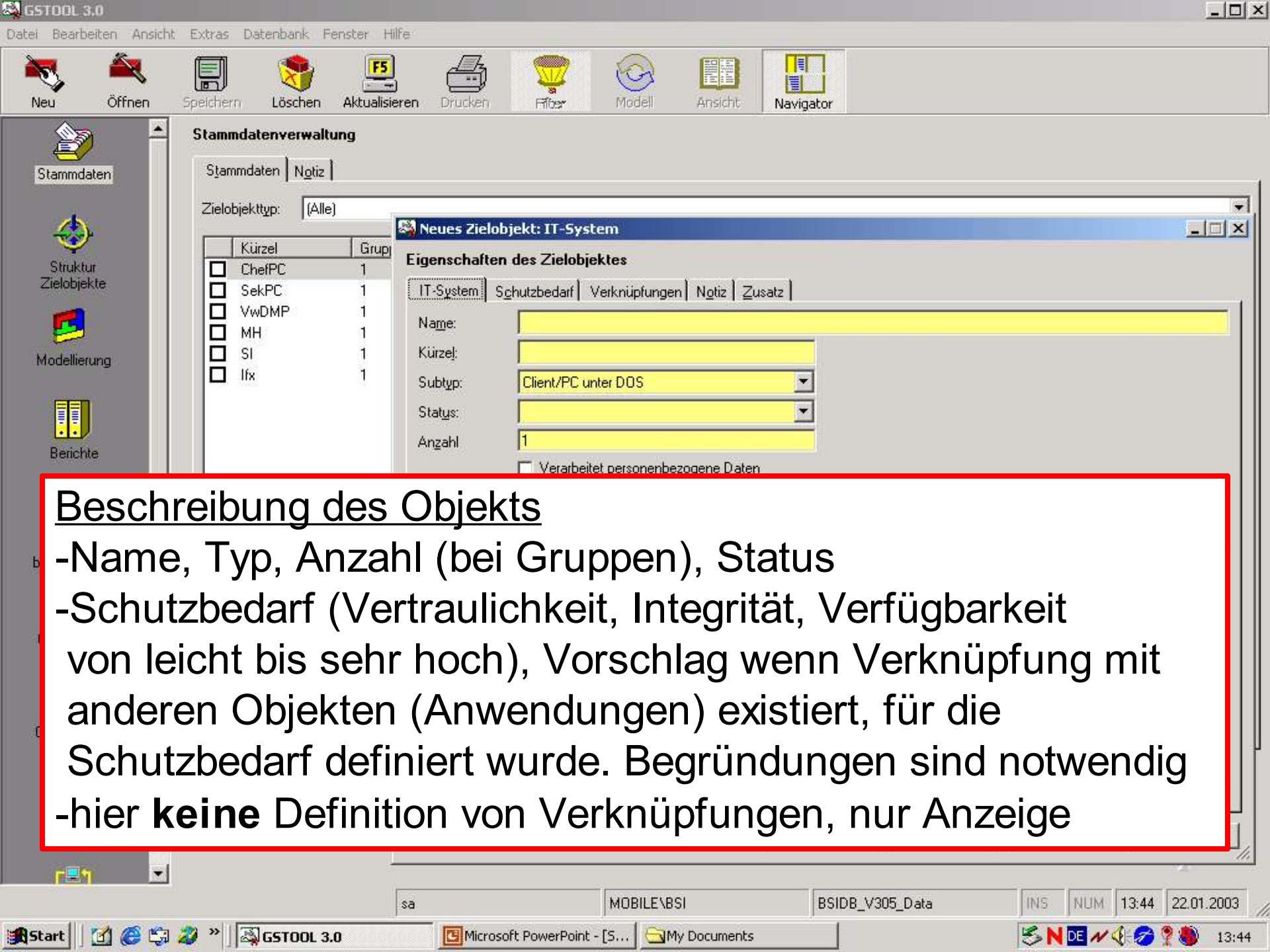
**Einzellizenz 887,40 EUR, 50%
Hochschulrabatt**

- **Stammdatenerfassung**
- **Strukturierung der Objekte, Definition von Abhängigkeiten (z.B. Anwendung->System)**
- **Modellierung: Bearbeitung der Einzelmaßnahmen**
- **Anpassung des Maßnahmenkatalogs an eigene Bedürfnisse**



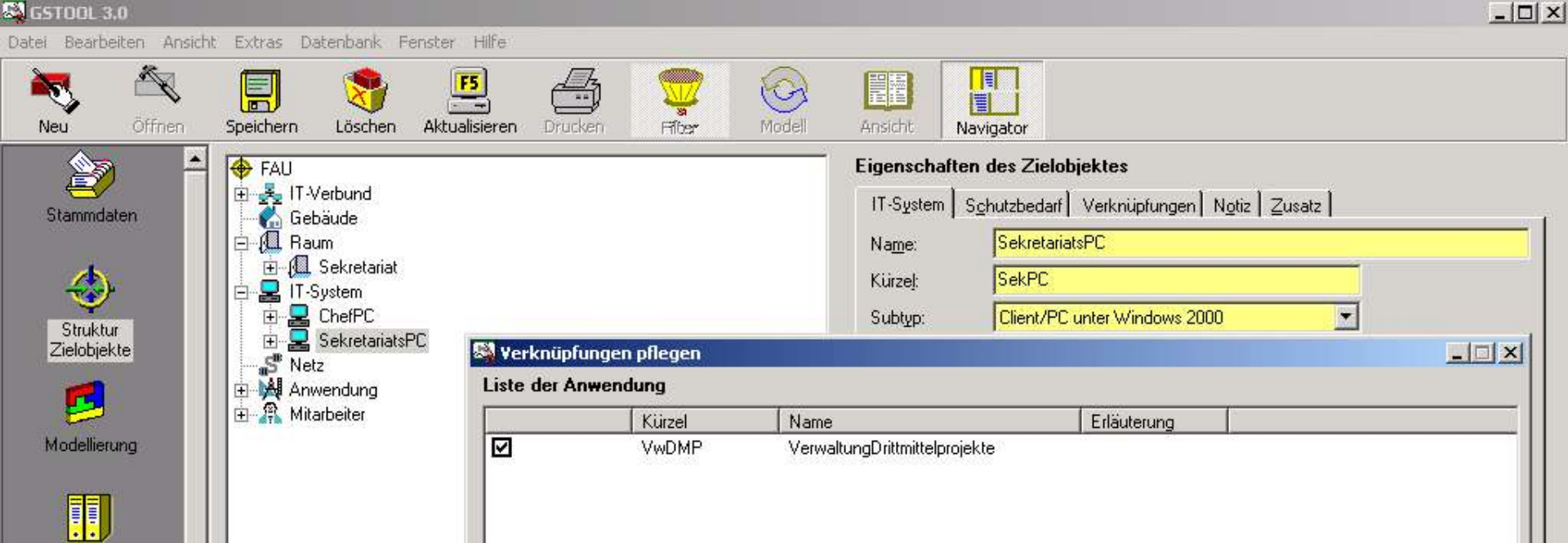
Anlegen neuer Objekte

- leeres Objekt des gleichen Typs wie markiert
- neues Objekt des gleichen Typs mit Datenübernahme
- Auswahl des Objekttyps (System, Anwendung, Personen...)



Beschreibung des Objekts

- Name, Typ, Anzahl (bei Gruppen), Status
- Schutzbedarf (Vertraulichkeit, Integrität, Verfügbarkeit von leicht bis sehr hoch), Vorschlag wenn Verknüpfung mit anderen Objekten (Anwendungen) existiert, für die Schutzbedarf definiert wurde. Begründungen sind notwendig
- hier **keine** Definition von Verknüpfungen, nur Anzeige



Struktur der Zielobjekte

- Auswahl Objekt, rechte Maustaste, Verknüpfungen pflegen
- Auswahl des Typs des zu verknüpfenden Objekts, Markierung
- Schutzbedarf wird **als Empfehlung** von dem verknüpften Objekt übernommen, muss aber **manuell** für das Objekt eingegeben und begründet werden
- Schutzbedarf bleibt bei Änderung/Auflösung der Verknüpfung **bestehen!!**



Modellierung

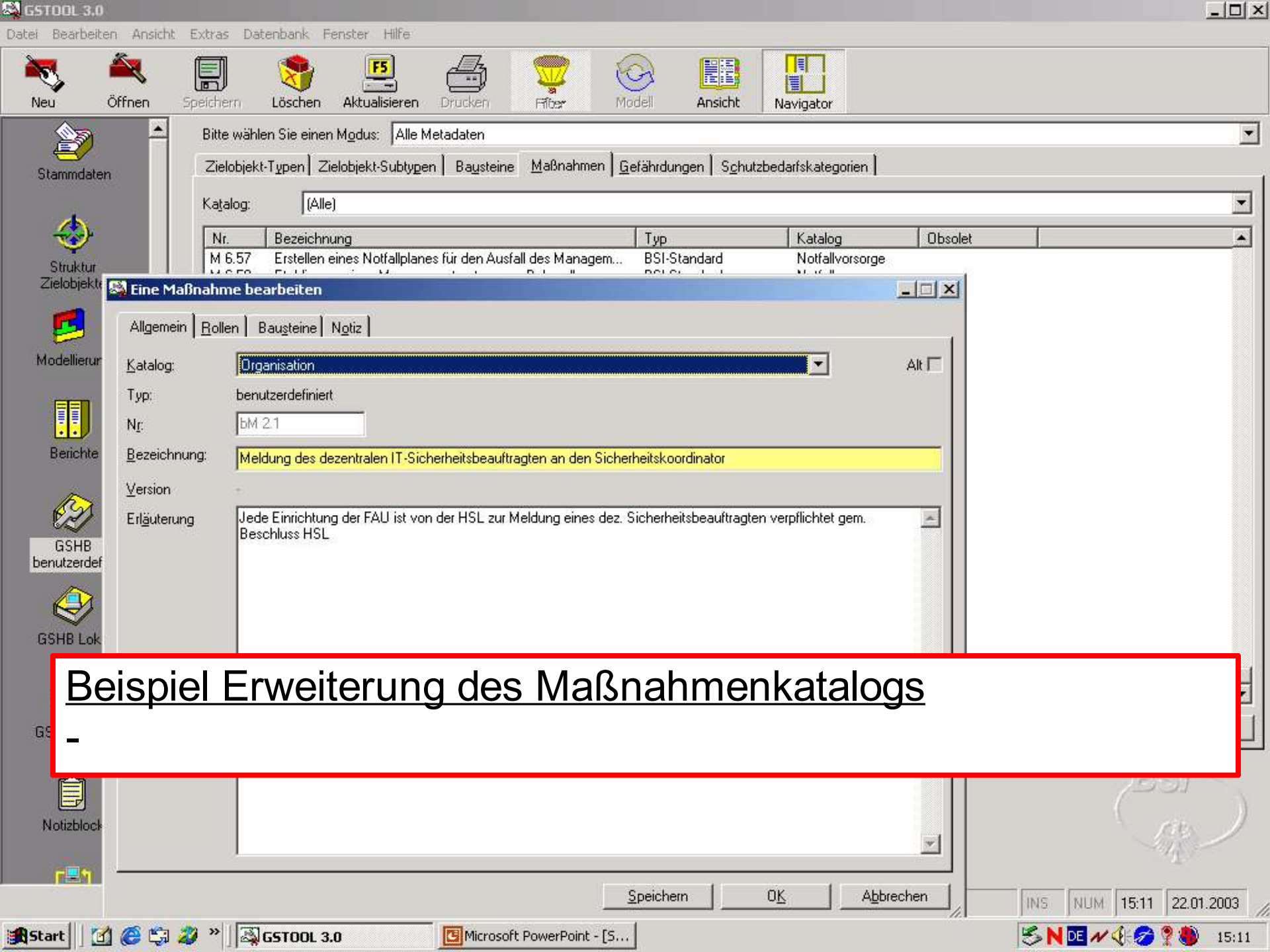
- Ansicht Objektmodell oder Schichtenmodell (Ansicht-Darstellung)
- Filter können definiert werden
- Maßnahmen sind für unterschiedliche Zertifizierungsgrade gekennzeichnet (A Selbsterklärung ohne Bestätigung, B S. mit Bestätigung, C Zertifikat nach Auditierung)
- jede Maßnahme muß einzeln bearbeitet werden!

Das GST kann durch Benutzer an eigene Bedürfnisse angepasst werden

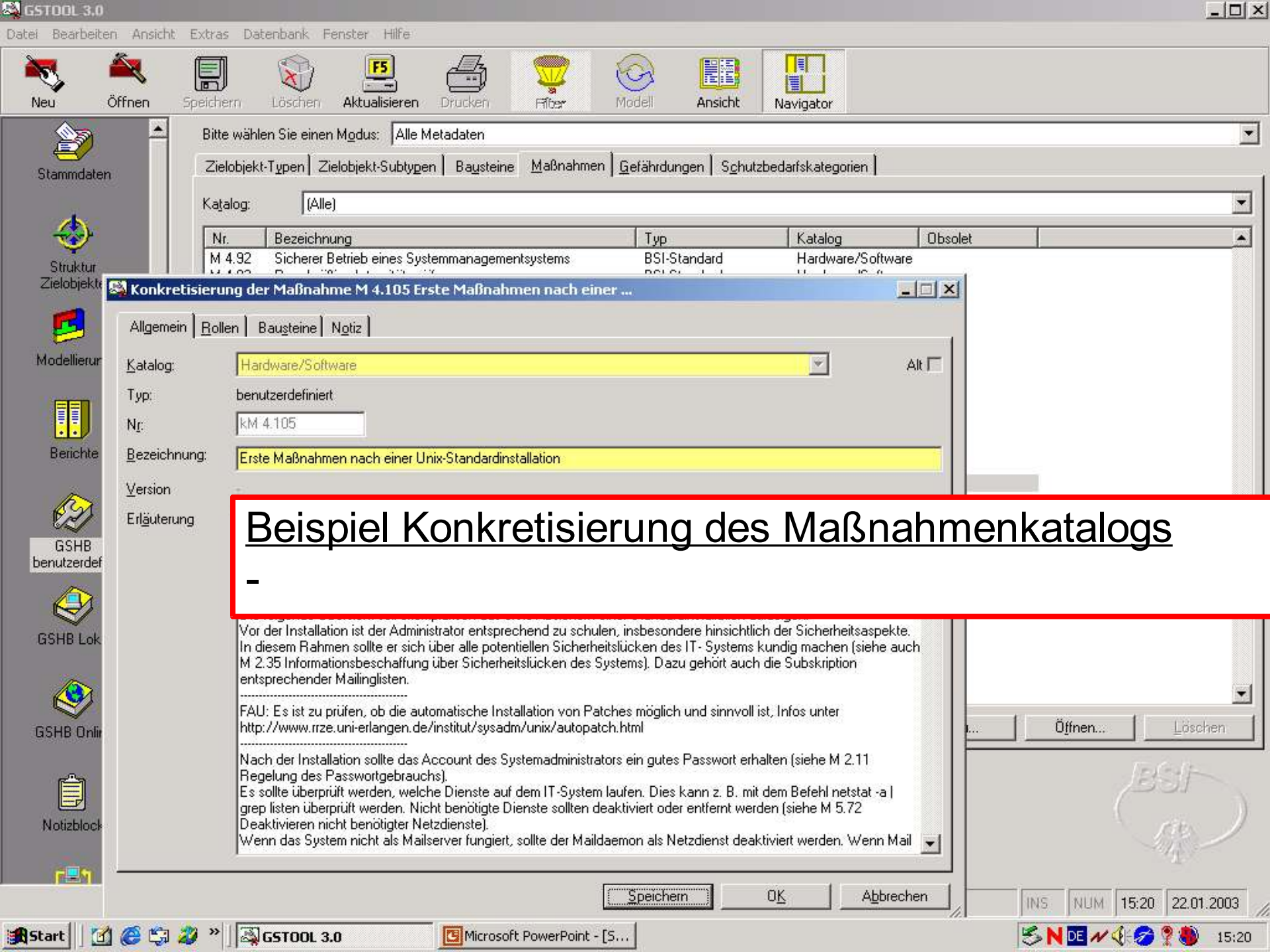
- **Maßnahmen: Standardmaßnahmen können konkretisiert oder eigene eingegeben werden**
- **Bausteine (Zusammenstellungen fachlicher Maßnahmen) können erweitert, vorhandene konkretisiert werden**
- **Zielobjekttypen können neu definiert werden**

Nicht verändert werden kann:

- **Gefährungen (nur durch BSI über Update)**
- **Standard-Maßnahmenkatalog (ausser Erweiterung/Konkretisierung), d.h. keine Einschränkungen möglich!**



Beispiel Erweiterung des Maßnahmenkatalogs



Beispiel Konkretisierung des Maßnahmenkatalogs

Vor der Installation ist der Administrator entsprechend zu schulen, insbesondere hinsichtlich der Sicherheitsaspekte. In diesem Rahmen sollte er sich über alle potentiellen Sicherheitslücken des IT- Systems kundig machen (siehe auch M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems). Dazu gehört auch die Subskription entsprechender Mailinglisten.

FAU: Es ist zu prüfen, ob die automatische Installation von Patches möglich und sinnvoll ist. Infos unter <http://www.rze.uni-erlangen.de/institut/sysadm/unix/autopatch.html>

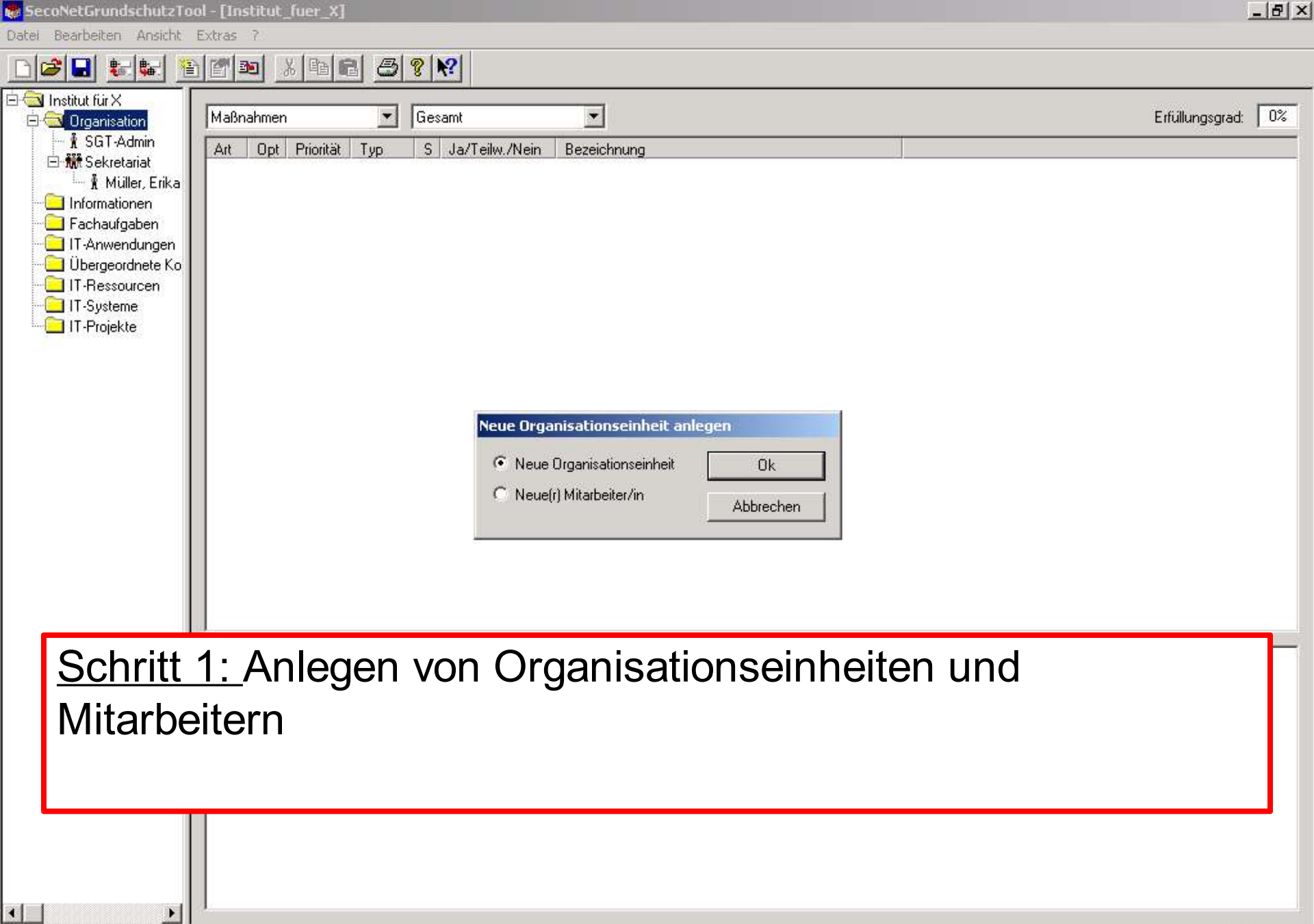
Nach der Installation sollte das Account des Systemadministrators ein gutes Passwort erhalten (siehe M 2.11 Regelung des Passwortgebrauchs).

Es sollte überprüft werden, welche Dienste auf dem IT-System laufen. Dies kann z. B. mit dem Befehl `netstat -a | grep listen` überprüft werden. Nicht benötigte Dienste sollten deaktiviert oder entfernt werden (siehe M 5.72 Deaktivieren nicht benötigter Netzdienste).

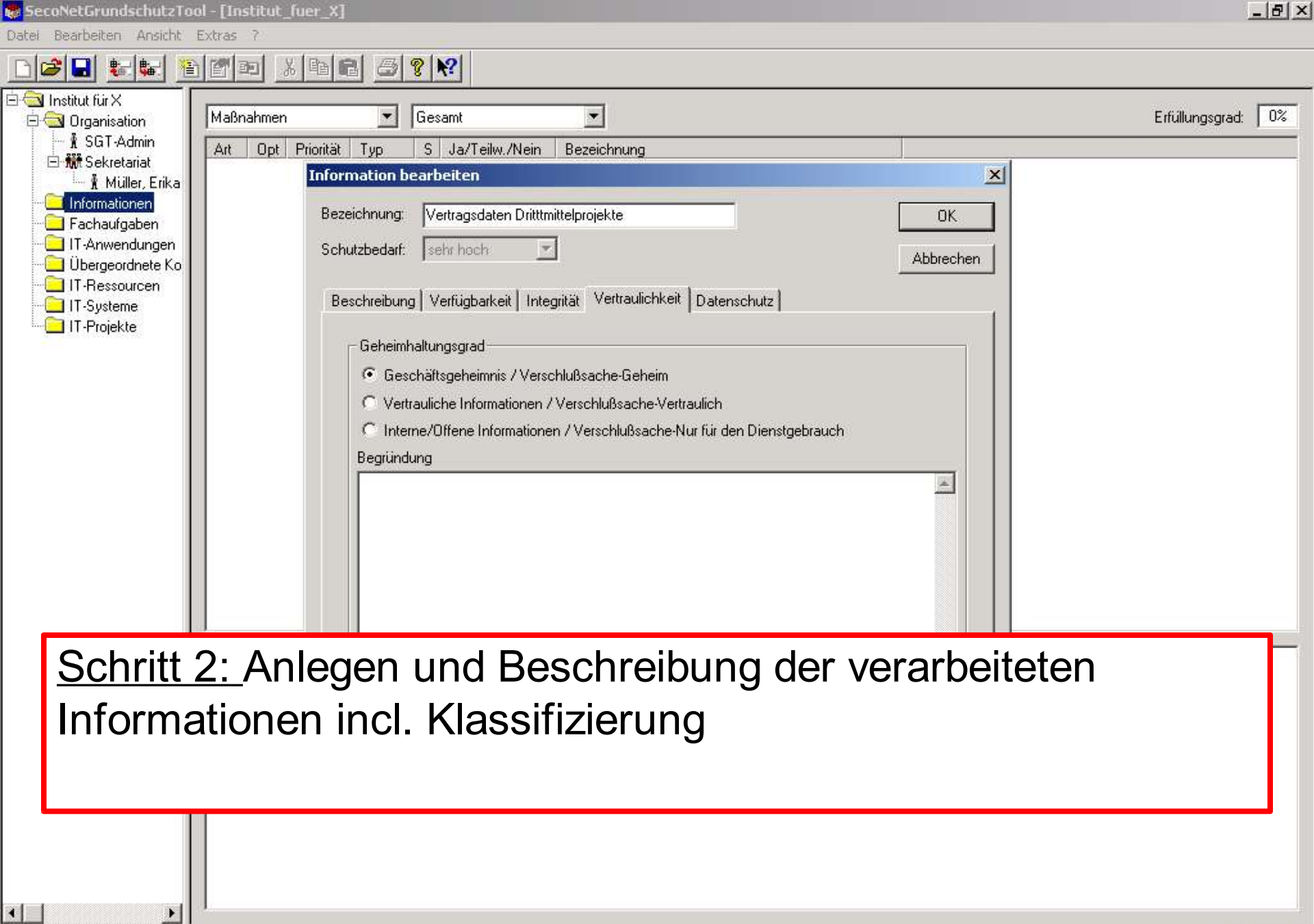
Wenn das System nicht als Mailserver fungiert, sollte der Maildaemon als Netzdienst deaktiviert werden. Wenn Mail

- **aktuelle Datenbasis seit wenigen Tagen erschienen (noch nicht auf hp)**
- **kostenlose Demoverision (2000) bei <http://www.seconet.de> (ohne Speichern und Drucken)**

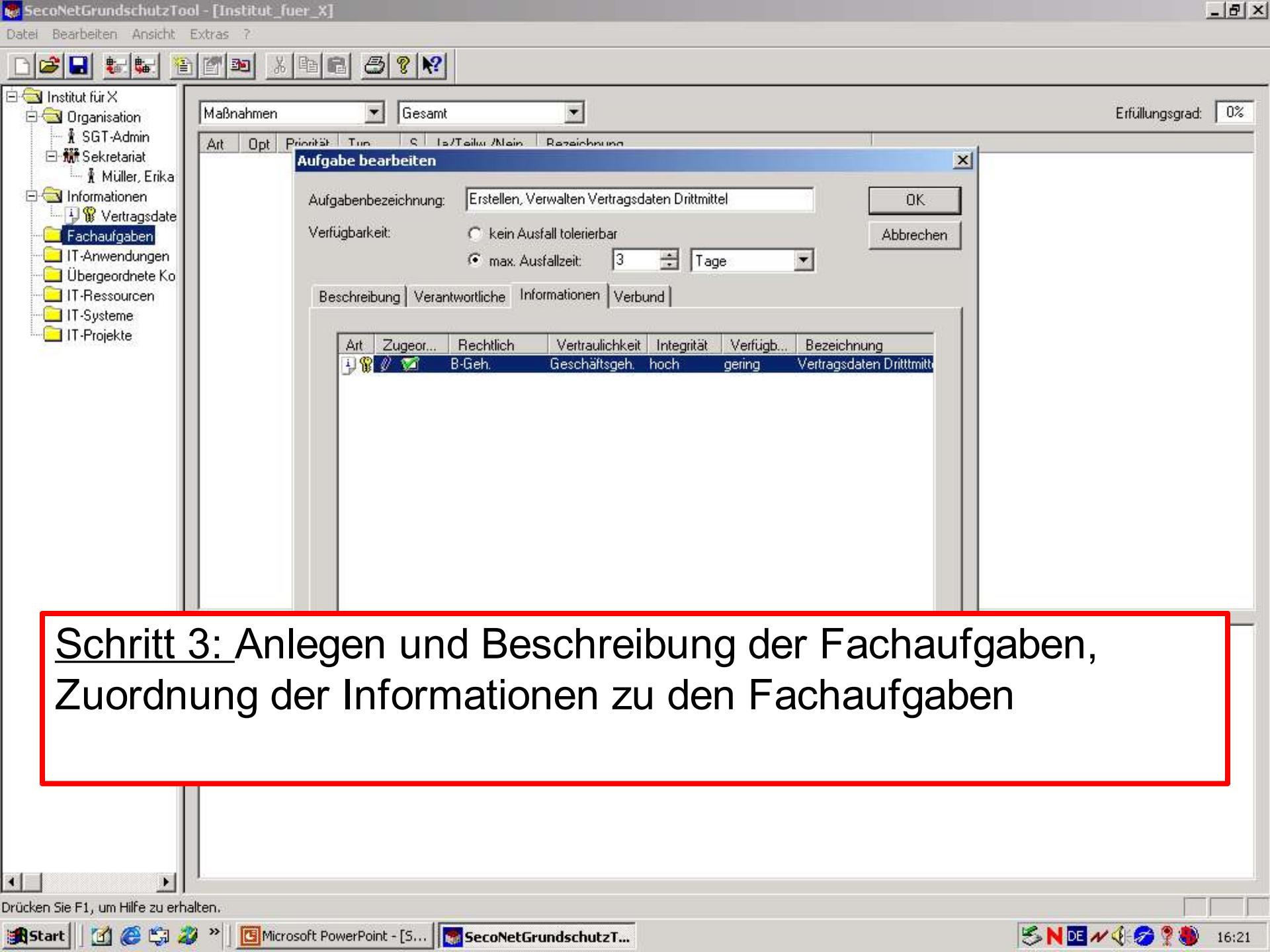
- **in den Funktionen ähnlich wie GST BSI**
- **ähnlich zu GST BSI,
Modellierung/Zuordnung von
Komponenten erfolgt beim Aufbau der
Datenbasis**
- **streng hierarchisch**



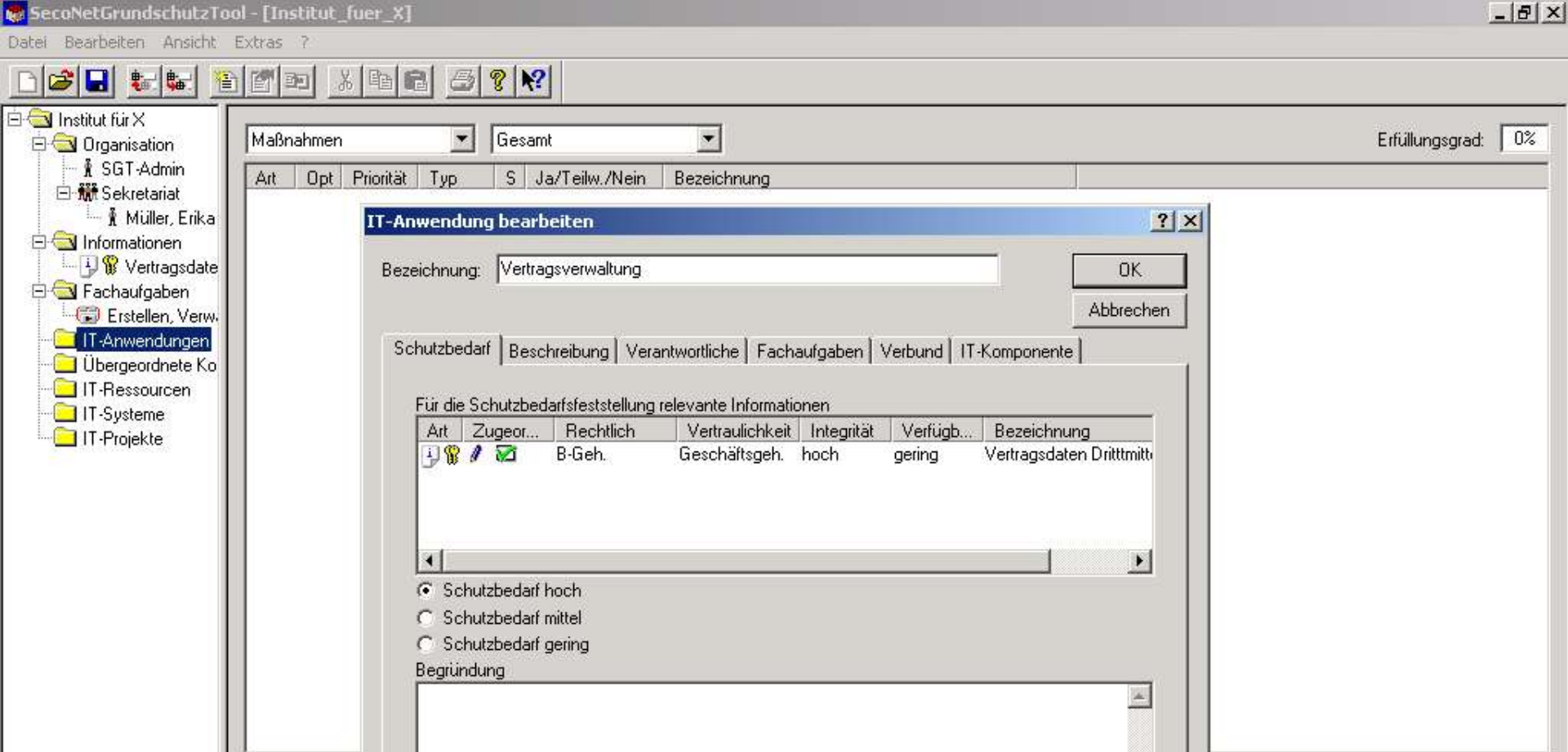
Schritt 1: Anlegen von Organisationseinheiten und Mitarbeitern



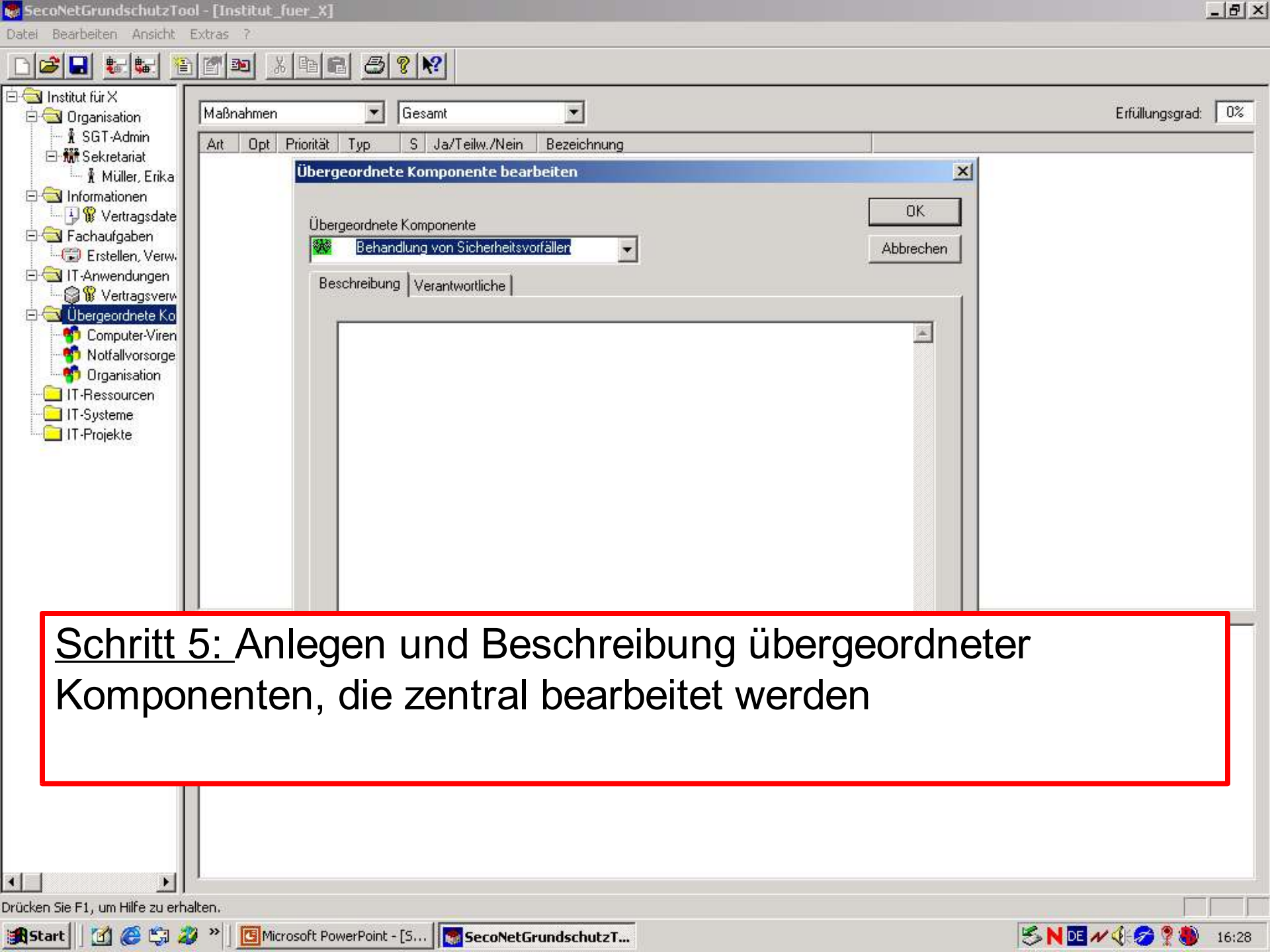
Schritt 2: Anlegen und Beschreibung der verarbeiteten Informationen incl. Klassifizierung



Schritt 3: Anlegen und Beschreibung der Fachaufgaben, Zuordnung der Informationen zu den Fachaufgaben



Schritt 4: Anlegen und Beschreibung der IT-Anwendungen, Zuordnung der Fachaufgaben, manuelle Definition des Schutzbedarfs (d.h. Änderungen der Klassifizierung von Informationen müssen hier u.U. nachgetragen werden)



Schritt 5: Anlegen und Beschreibung übergeordneter Komponenten, die zentral bearbeitet werden

SecoNetGrundschutzTool - [Institut_fuer_x]

Datei Bearbeiten Ansicht Extras ?

Maßnahmen Gesamt Erfüllungsgrad: 0%

Art Opt Priorität Typ S Ja/Teilw./Nein Bezeichnung

IT-Raum bearbeiten ? x

Bezeichnung:

OK

Abbrechen

Beschreibung Verantwortliche Bausteine

Bausteinauswahl

Art	Zuge...	Aktiv	Bezeichnung
	<input type="checkbox"/>		Büorraum
	<input type="checkbox"/>		Datenträgerarchiv
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Raum für technische Infrastruktur
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Schutzschränke(M-G-Tabelle f.Raum)
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Serverraum
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Verkabelung für Räume

Schritt 6: Anlegen der Ressourcen: Räume

SecoNetGrundschutzTool - [Institut_fuer_X]

Datei Bearbeiten Ansicht Extras ?

Maßnahmen Gesamt Erfüllungsgrad: 0%

Art Opt Priorität Typ S Ja/Teilw./Nein Bezeichnung

IT-Komponente bearbeiten

Bezeichnung: Sekretariats-PC im Betrieb geplant im Test

Leitbaustein: PC unter Windows NT

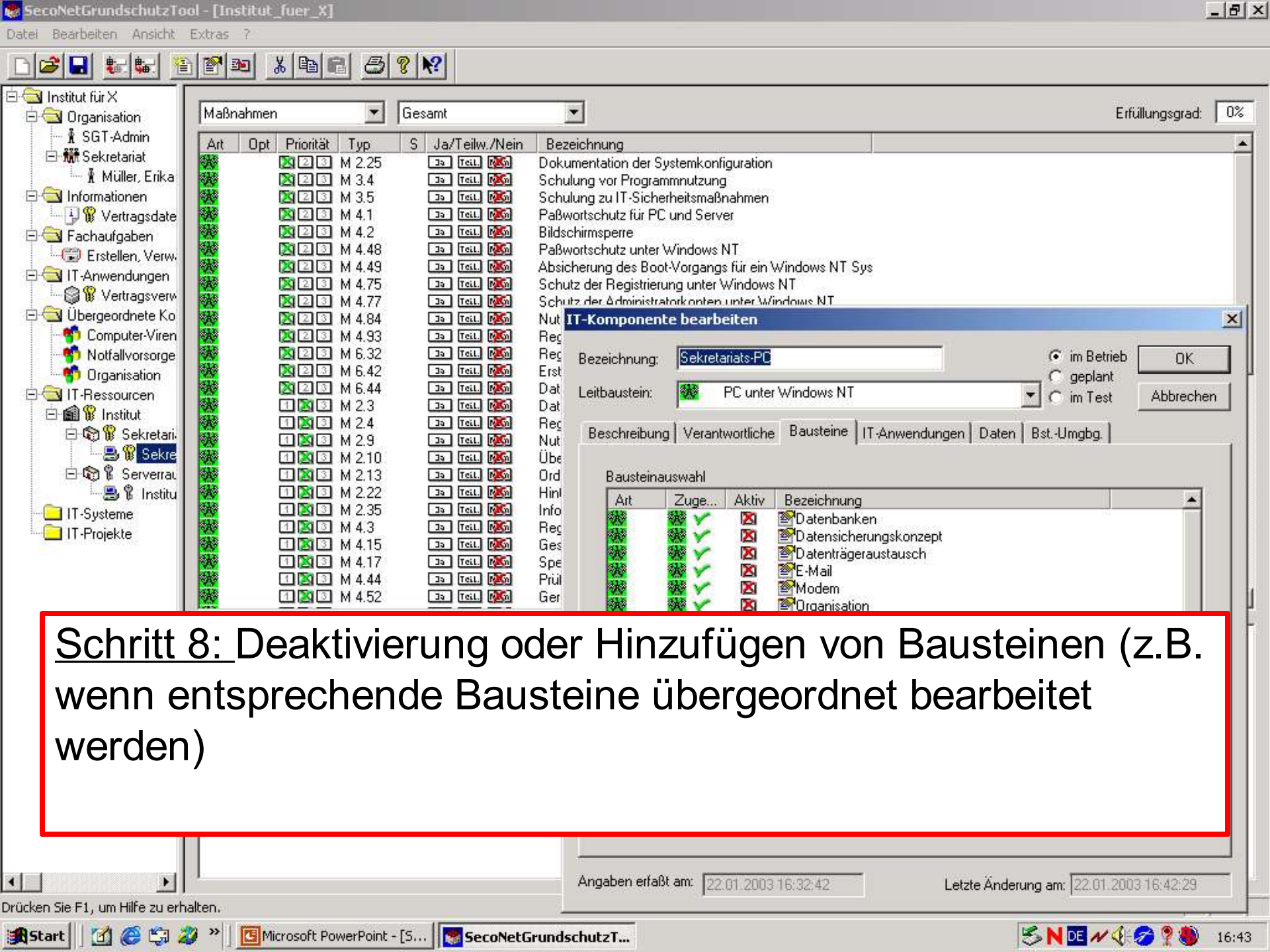
Beschreibung Verantwortliche Bausteine IT-Anwendungen Daten Bst.-Umgbg.

Bausteinauswahl

Art	Zuge...	Aktiv	Bezeichnung
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Datenbanken
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Datensicherungskonzept
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Datenträgeraustausch
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	E-Mail
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Modem
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Organisation
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Personal
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PC unter Windows NT
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Standardsoftware
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Allgemeines nicht vernetztes IT-System
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Anrufbeantworter
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Behandlung von Sicherheitsvorfällen
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Computer-Virenschutzkonzept
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	DOS-PC (1 Benutzer)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	DOS-PC (mehrere Benutzer)

Drücken Sie F1, um Hilfe zu erhalten.

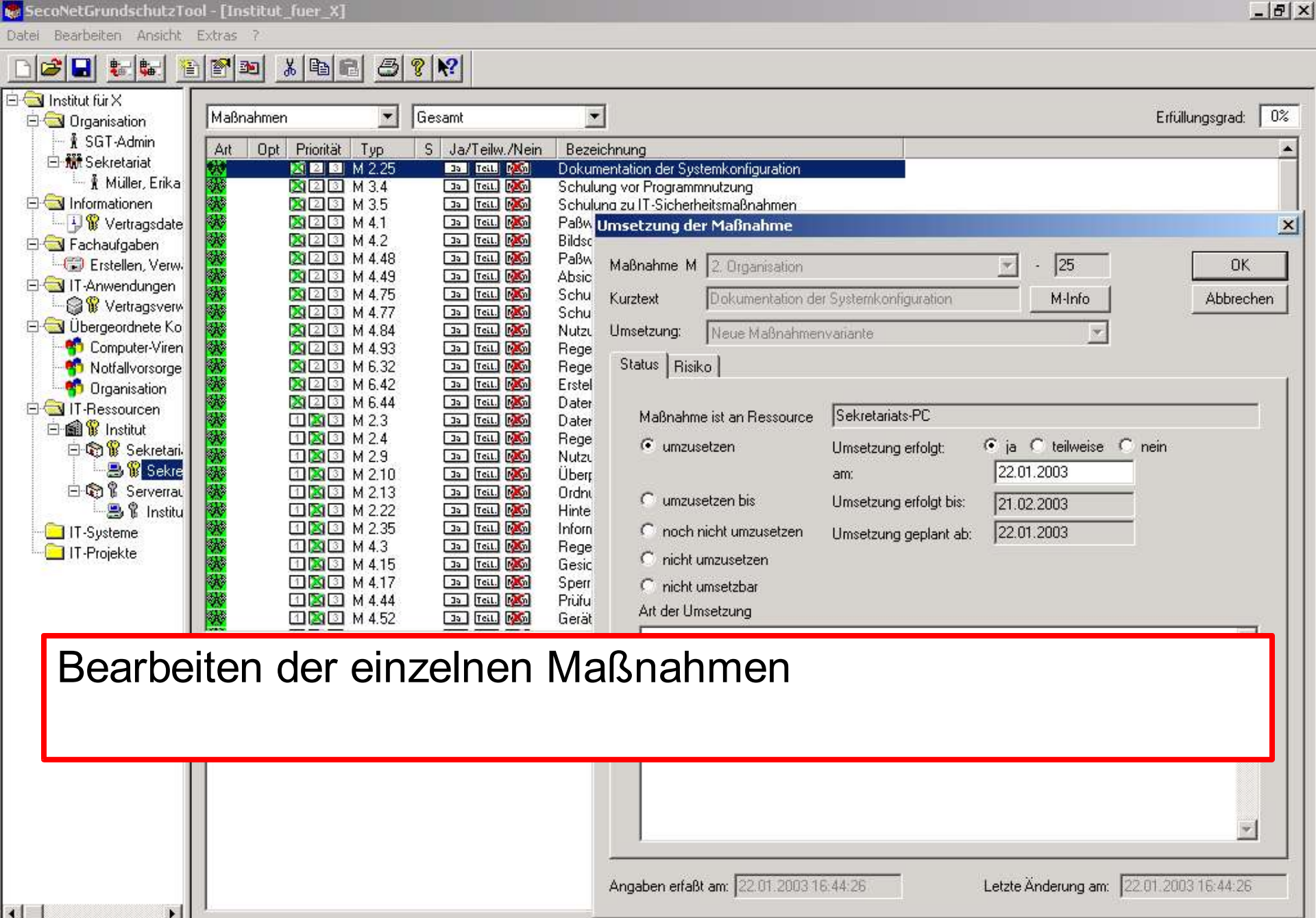
Schritt 7: Anlegen der Ressourcen: IT-Systeme (unterhalb von Räumen), Zuordnung von IT-Anwendungen



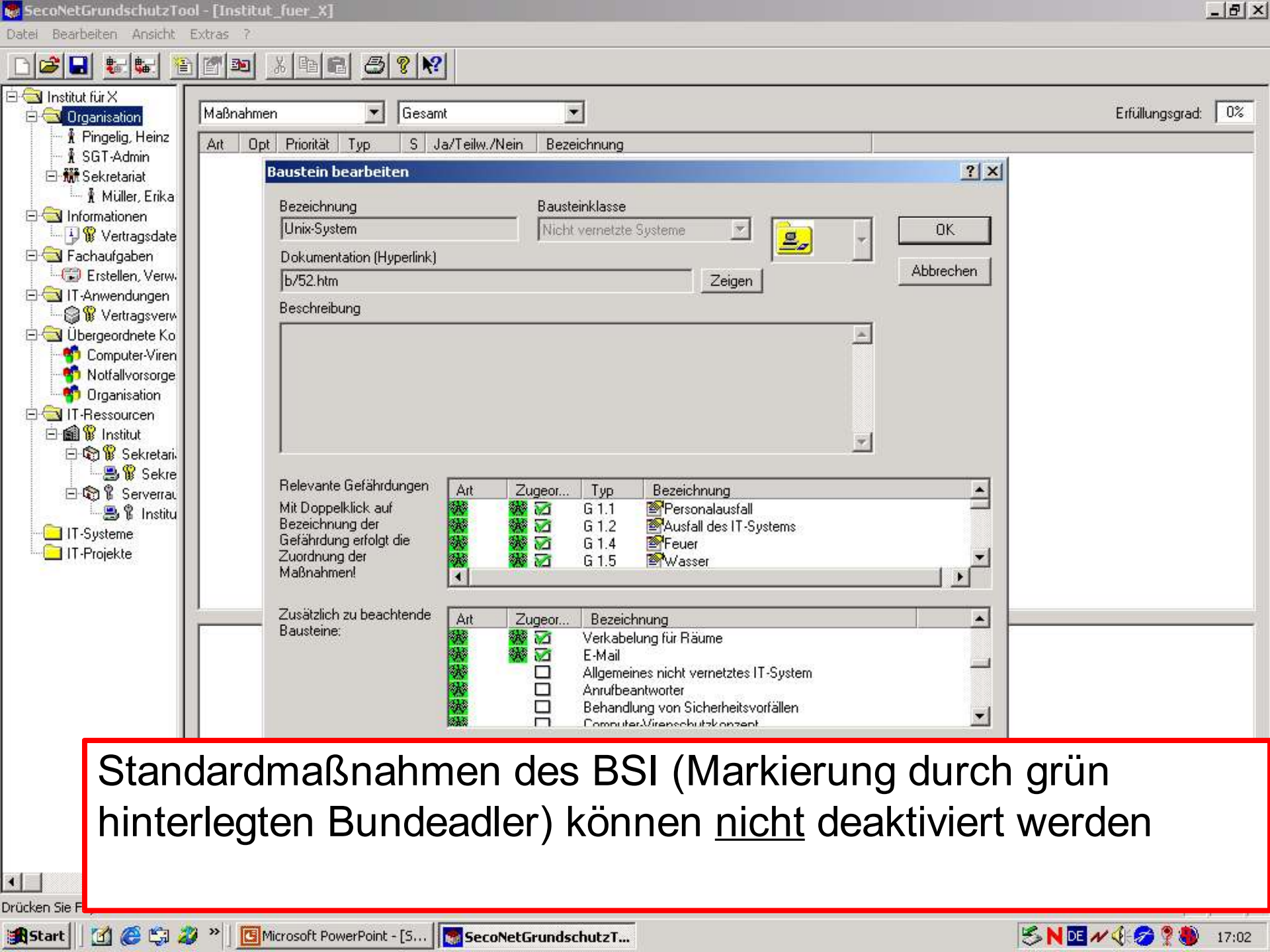
Schritt 8: Deaktivierung oder Hinzufügen von Bausteinen (z.B. wenn entsprechende Bausteine übergeordnet bearbeitet werden)

Angaben erfaßt am: 22.01.2003 16:32:42

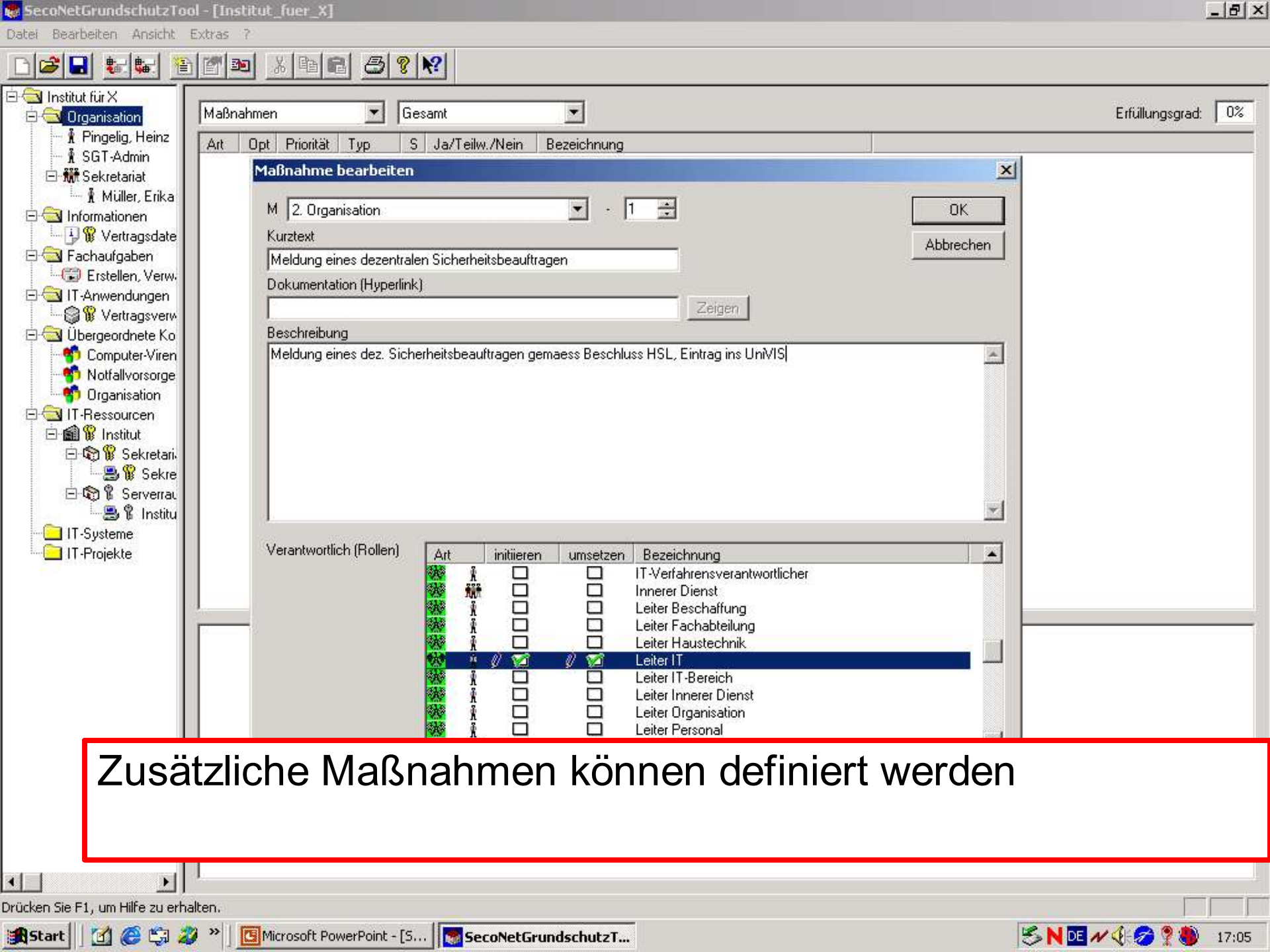
Letzte Änderung am: 22.01.2003 16:42:29



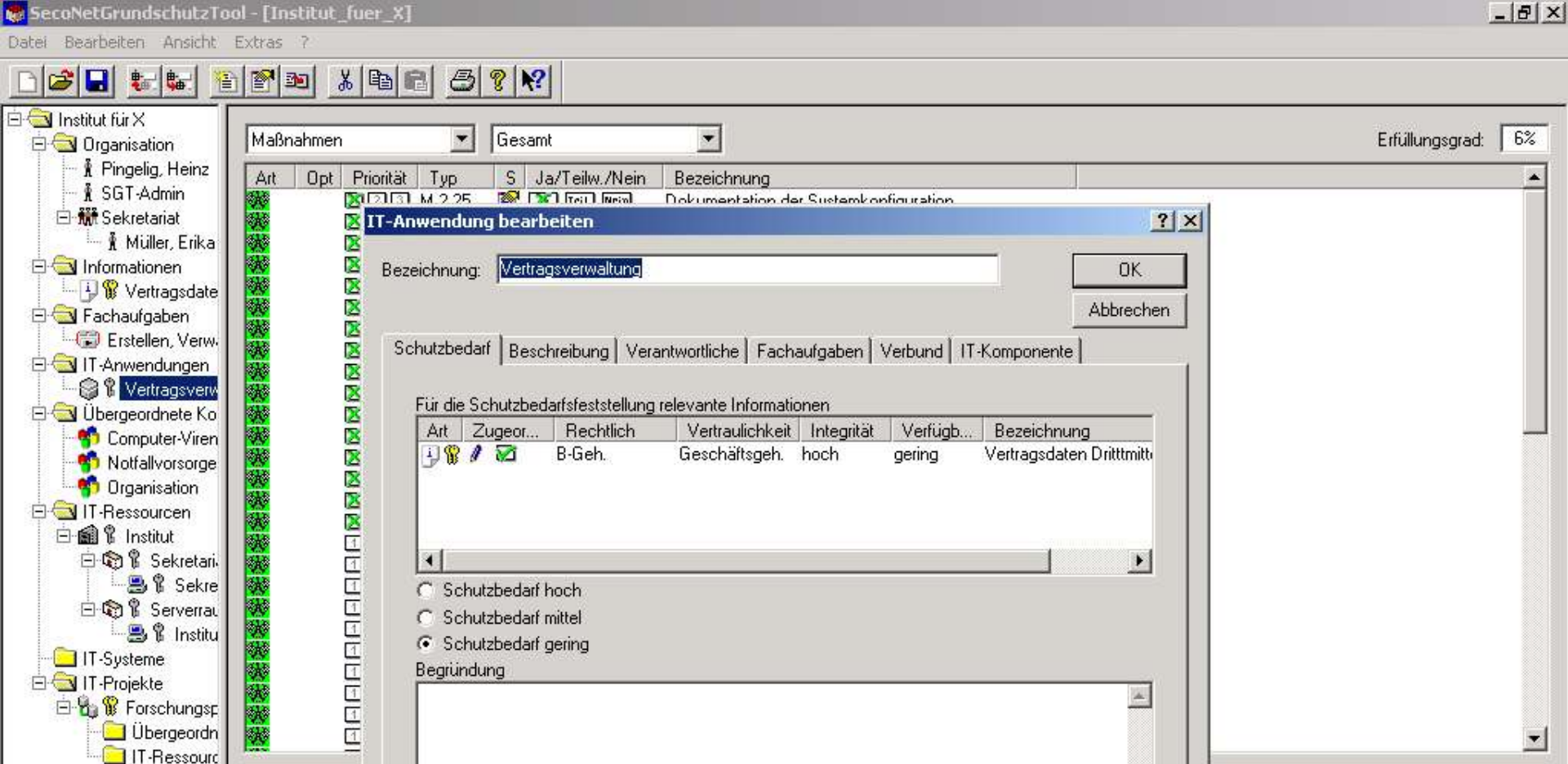
Bearbeiten der einzelnen Maßnahmen



Standardmaßnahmen des BSI (Markierung durch grün hinterlegten Bundeader) können nicht deaktiviert werden



Zusätzliche Maßnahmen können definiert werden



Änderungen an den Informationen wirken sich nicht automatisch auf die IT-Systeme aus, Änderung muss bei der Anwendung mitgezogen werden

- **da keine Kürzungen am Maßnahmenkatalog möglich sind für die grundlegenden Schutzmaßnahmen der FAU zu aufwändig**
- **sinnvoll bzw. notwendig, wenn eine Zertifizierung angestrebt wird**
- **gute Kenntnis des Grundschutzhandbuchs erforderlich**