SerNet

Der Modernisierte Grundschutz in verinice

verinice.XP 2018

Michael Flürenbrock

verinice Product Owner

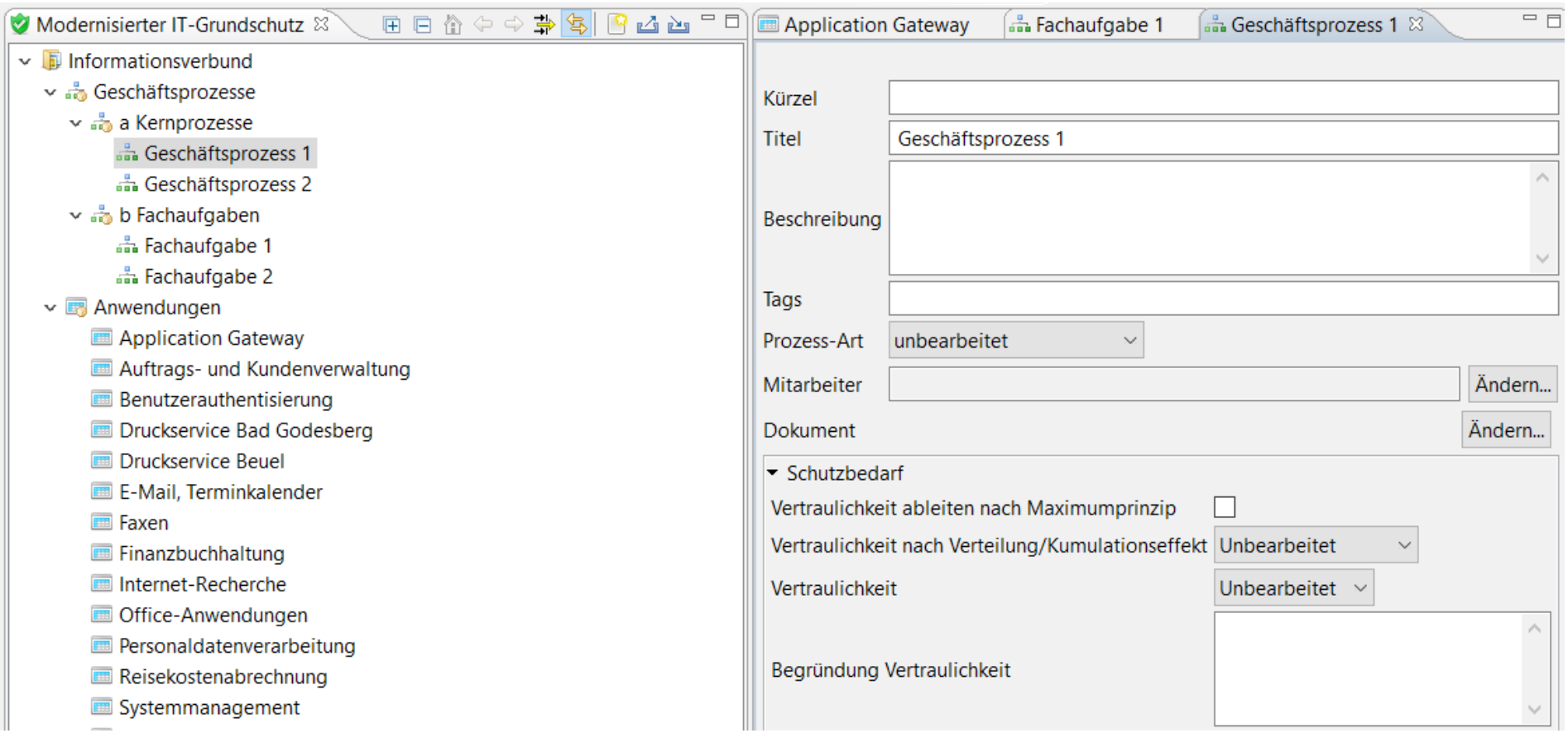
Ablauf im Modernisierten Grundschutz

SerNet

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- IT-Grundschutz-Check
- Risikoanalyse

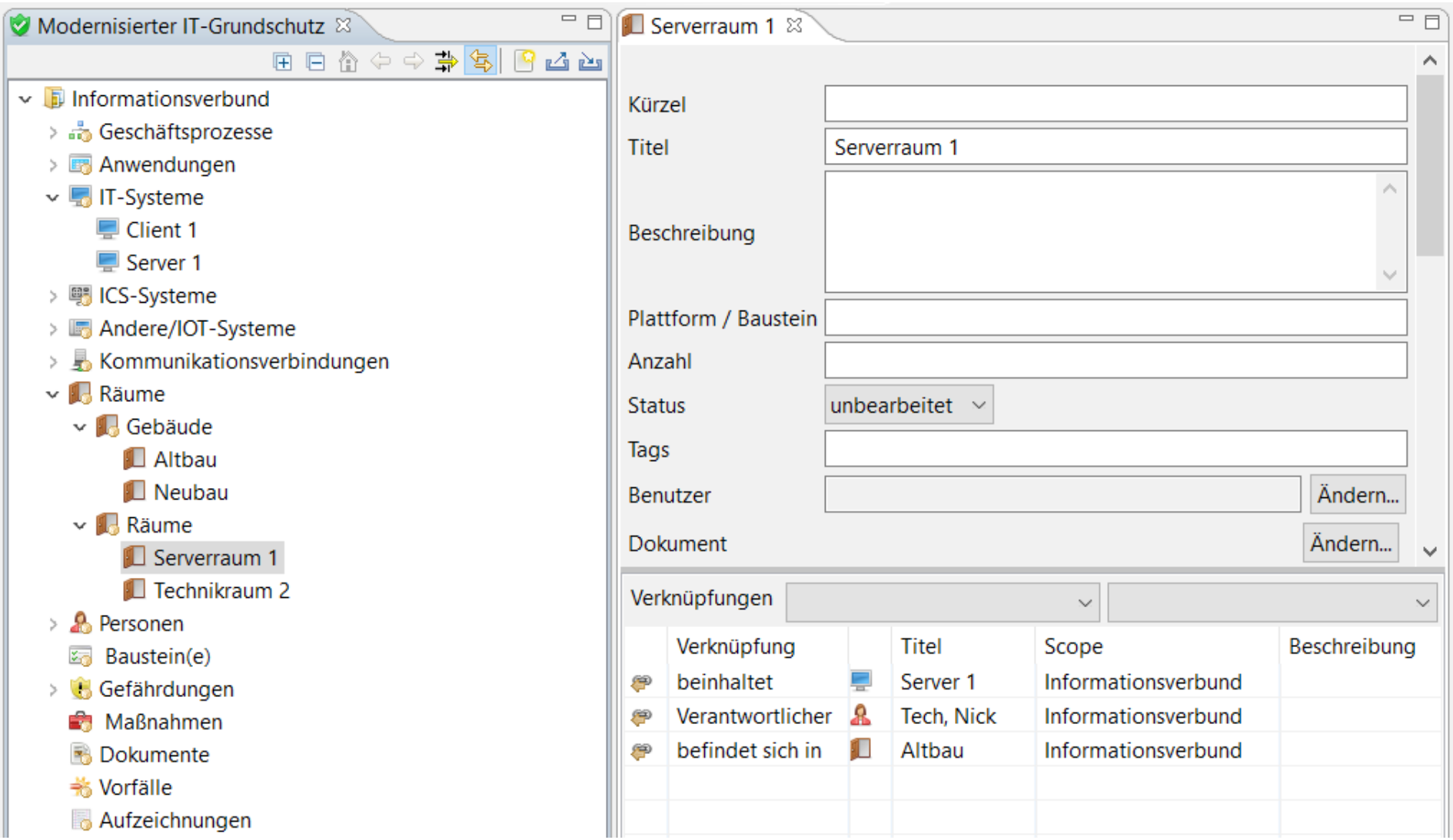
Strukturanalyse - Prozesse

SerNet



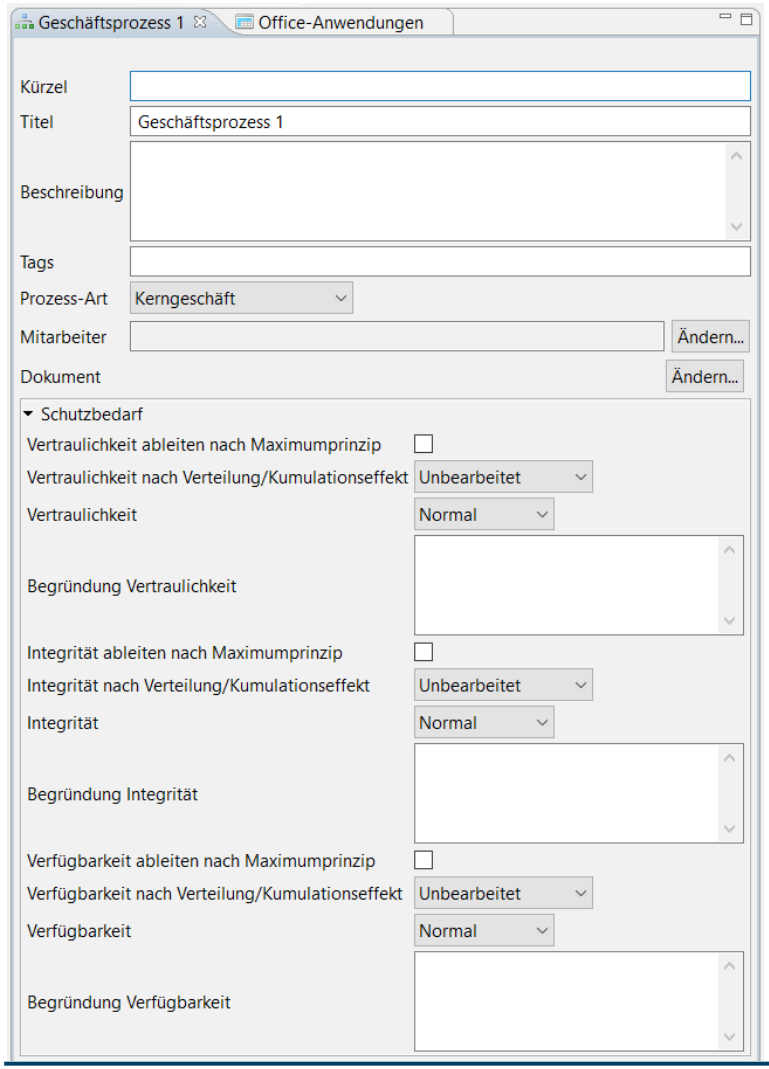
Strukturanalyse Zielobjekte

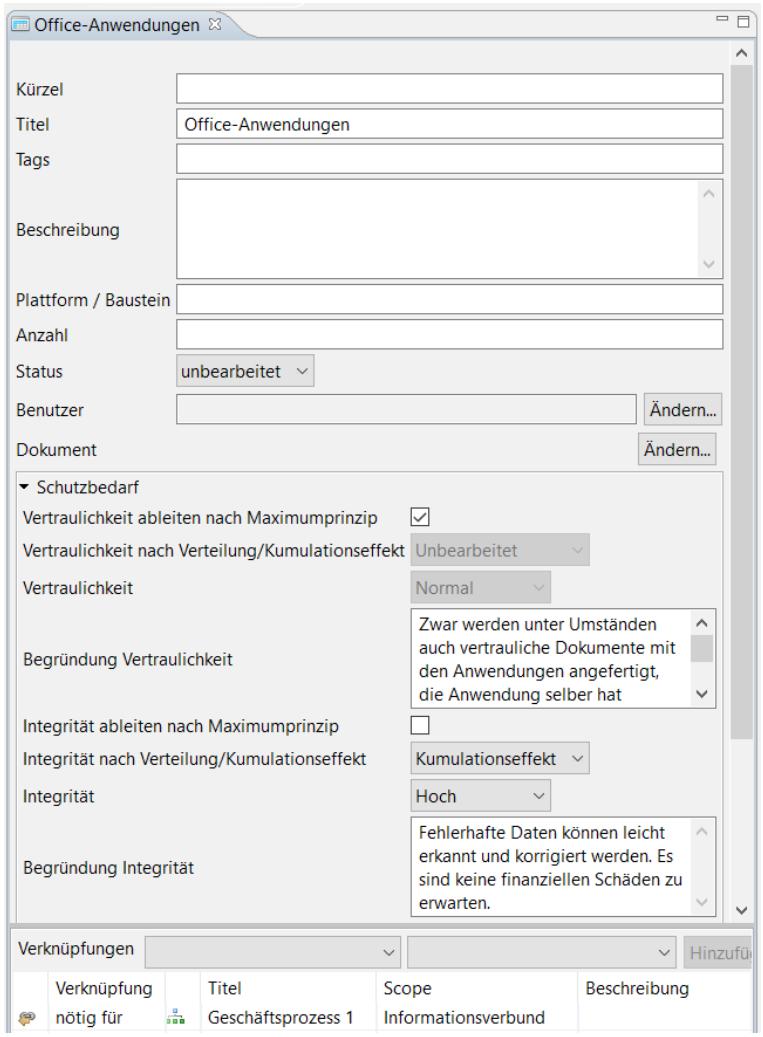
SerNet



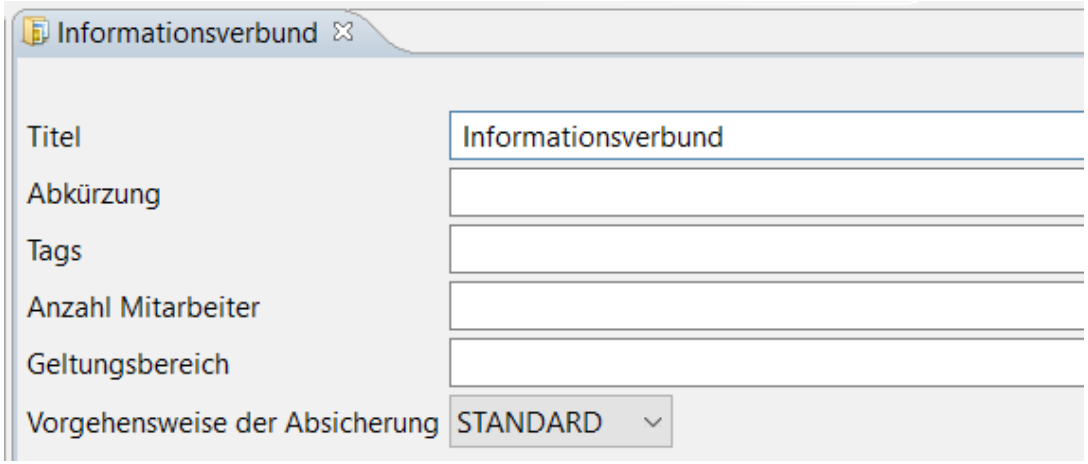
Schutzbedarfsfeststellung & -vererbung

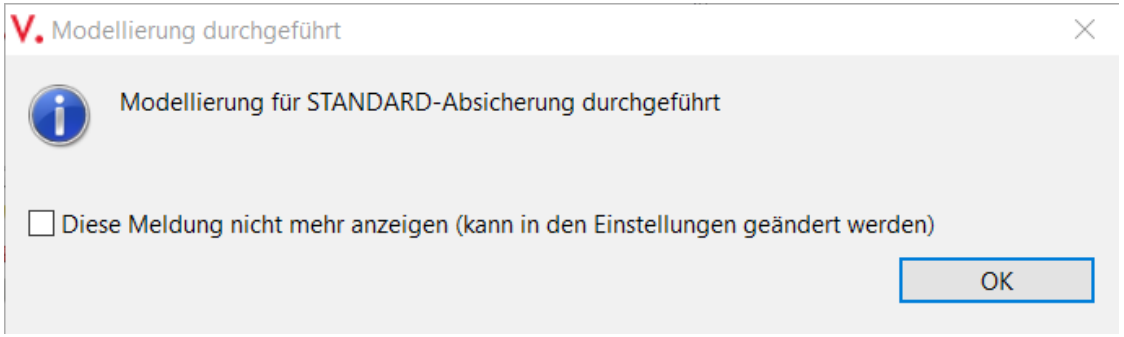
SerNet





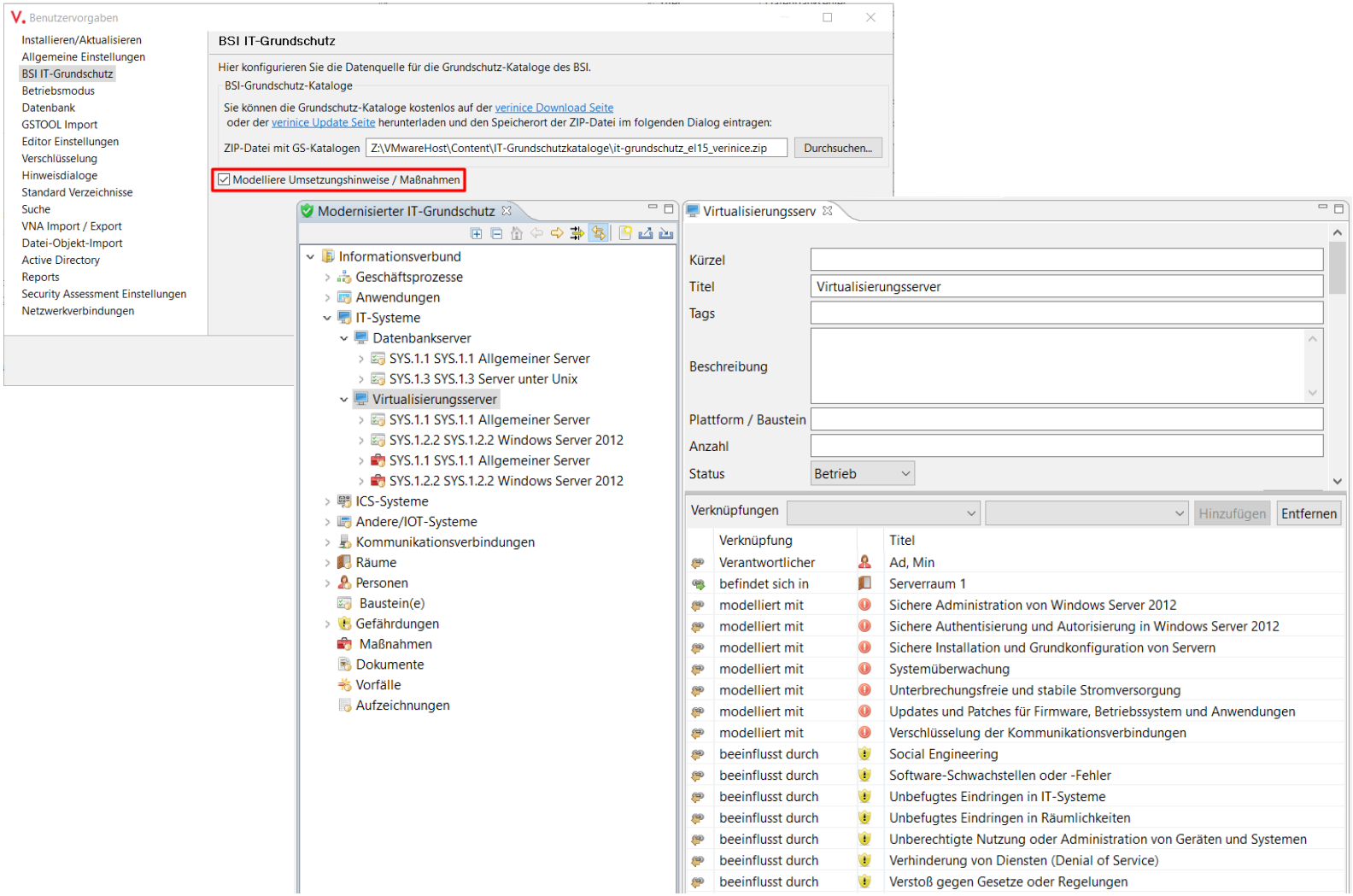
Modellierung – Vorgehensweise der Absicherung





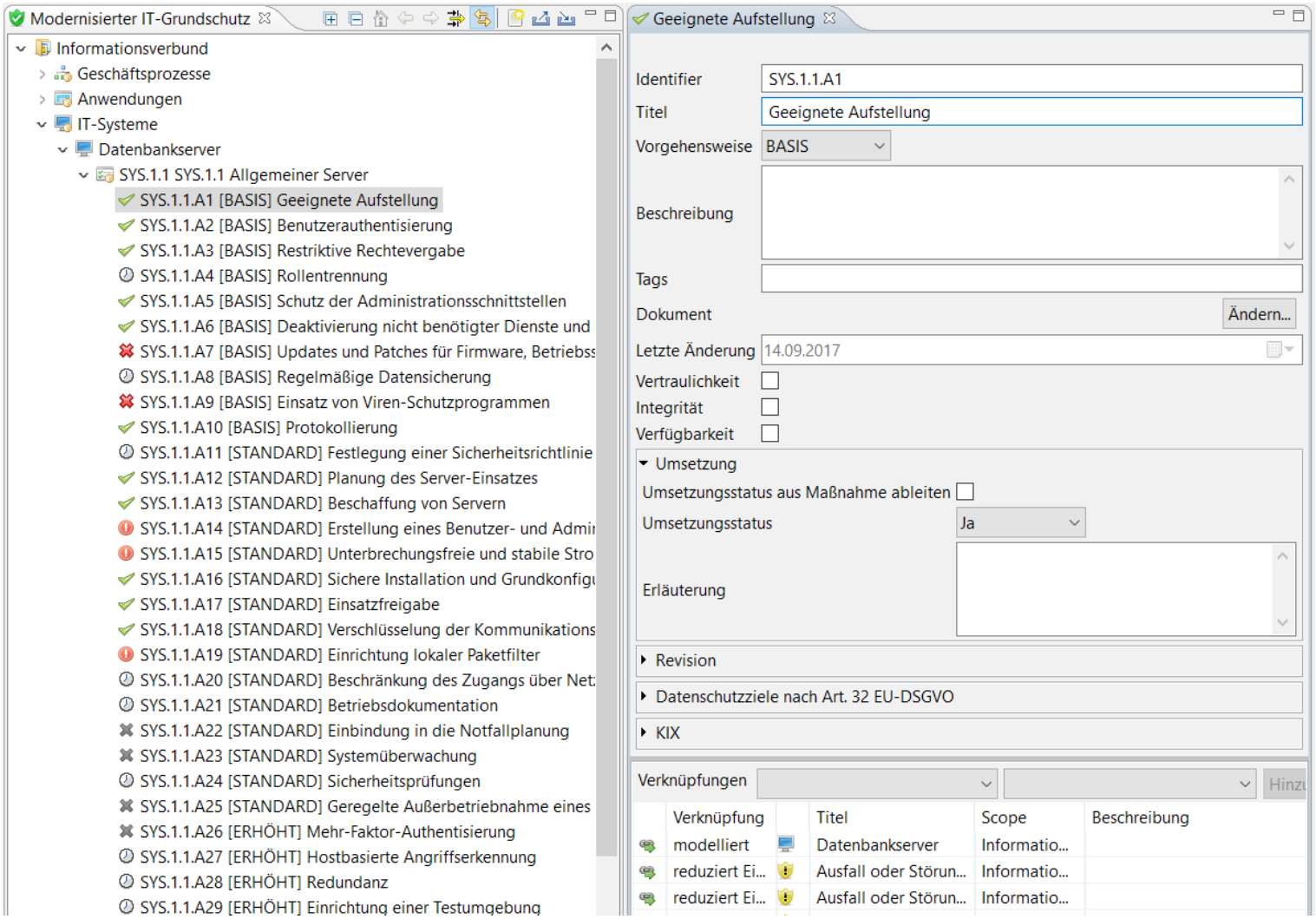
Modellierung – Anforderungen & Maßnahmen

SerNet



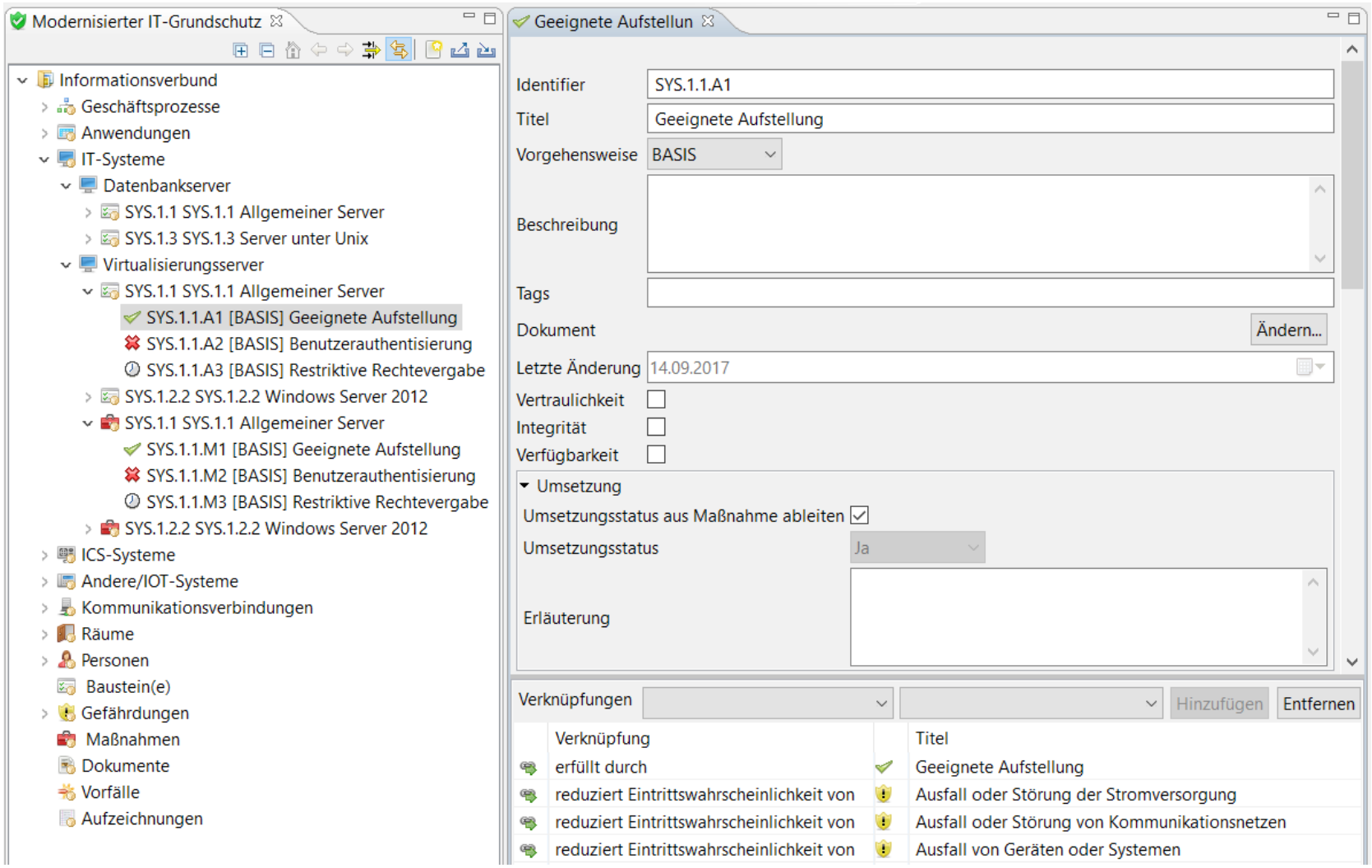
Modellierung - Umsetzungsstatus

SerNet



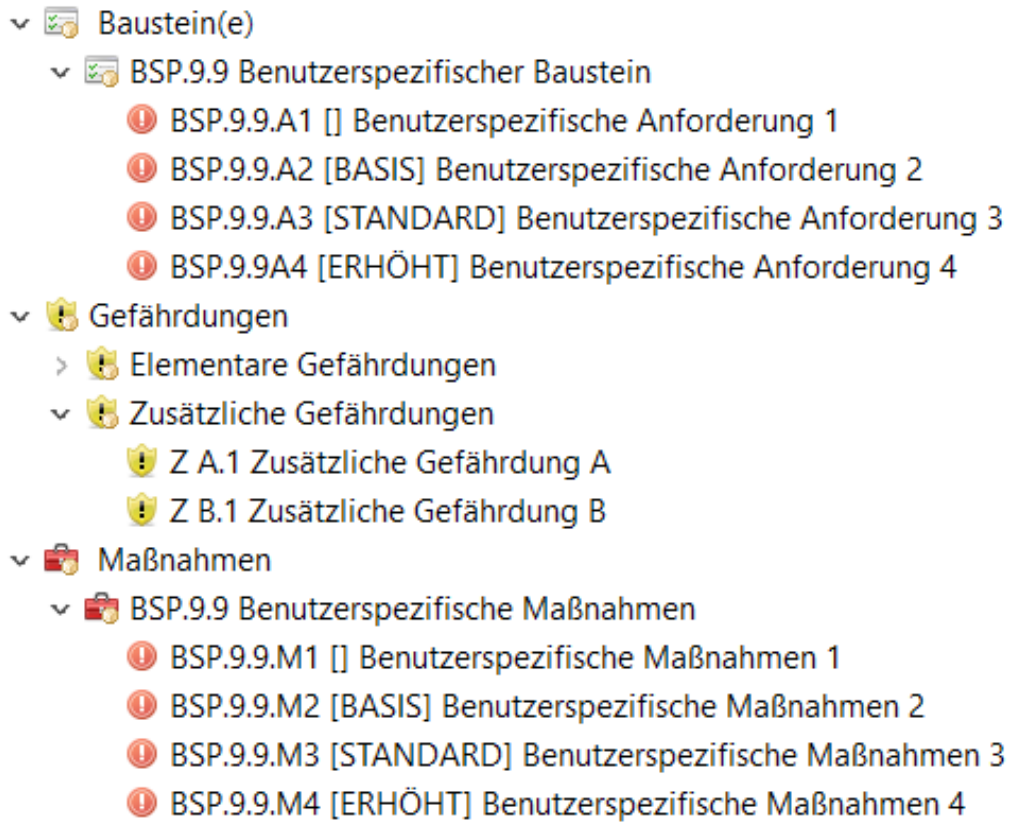
Modellierung – Umsetzungsstatus ableiten

SerNet



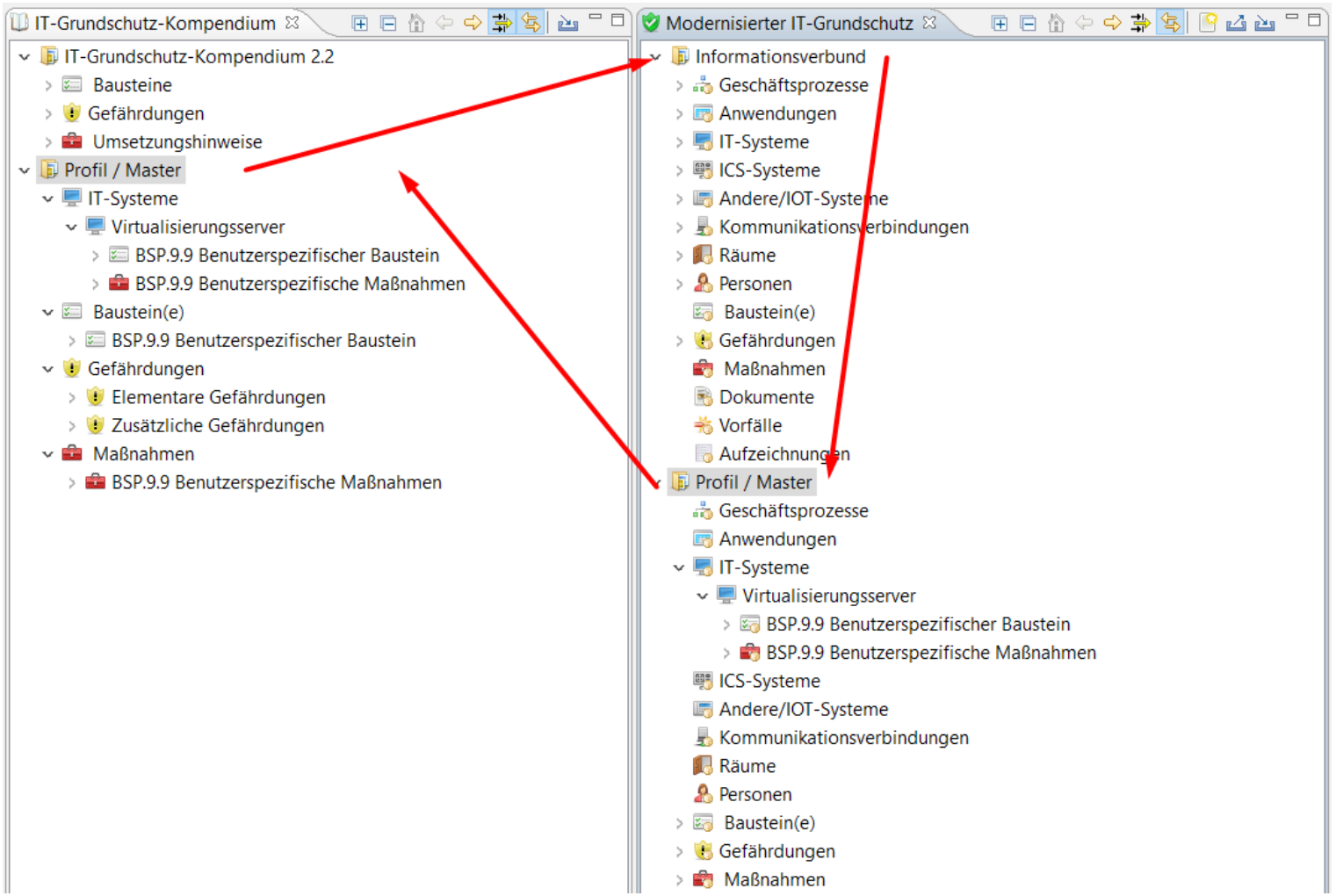
Modellierung - Benutzerdefinierte Bausteine

SerNet



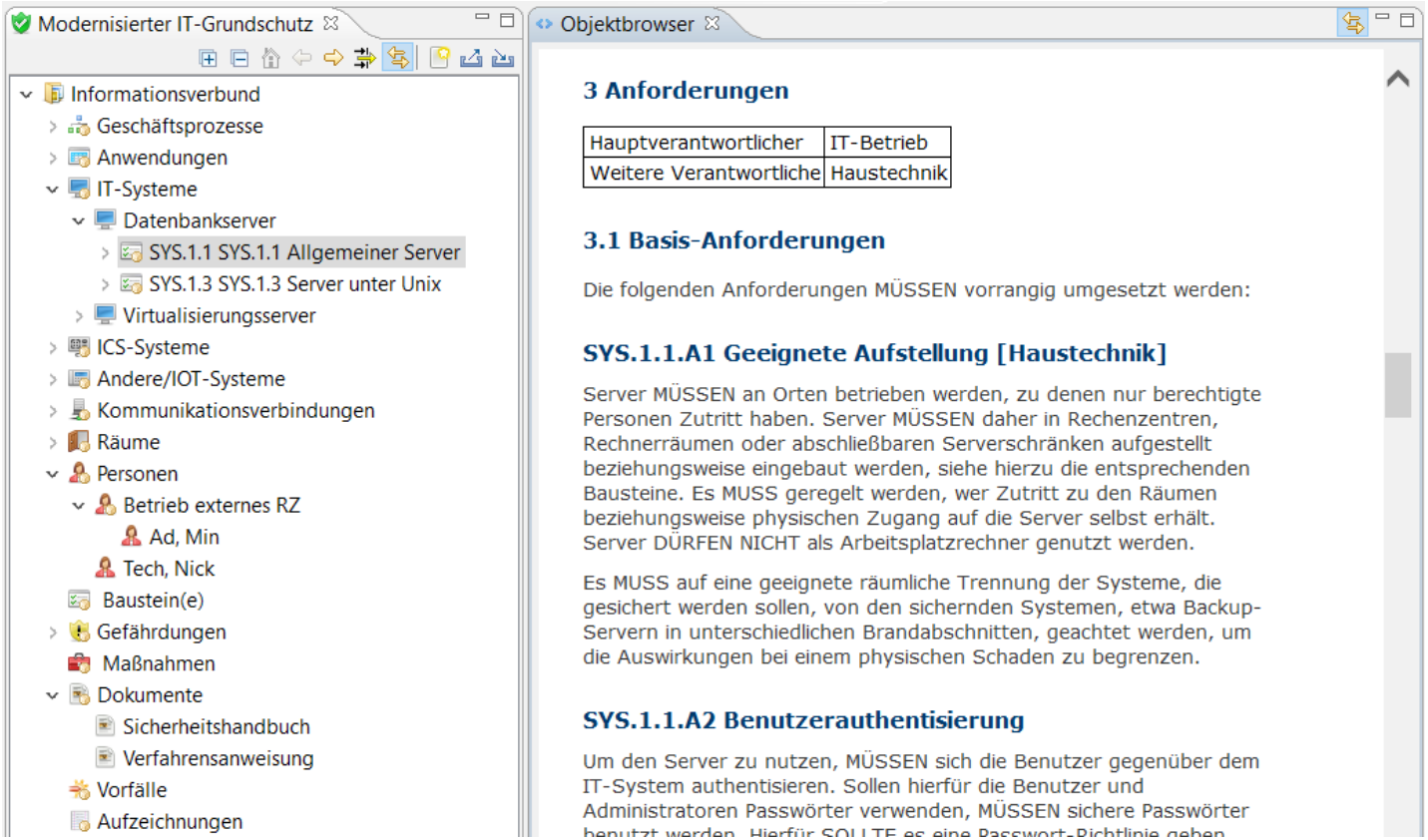
Modellierung – Profile / Templates

SerNet



IT-Grundschutz-Check - Vorarbeiten

SerNet



- Dokumentation sichten
- Externe Stellen identifizieren
- Hauptansprechpartner identifizieren

IT-Grundschutz-Check - Soll-Ist-Vergleich

SerNet

„… als Antworten bezüglich des Umsetzungsstatus der einzelnen **Anforderungen** kommen folgende Aussagen in Betracht:“

entbehrlich - Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil…

ja - Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt.

teilweise - Die Anforderung wurde nur teilweise umgesetzt. => *Maßnahmen unvollständig, unwirksam oder unangemessen umgesetzt?*

nein - Die Anforderung wurde noch nicht erfüllt, also geeignete Maßnahmen sind größtenteils noch nicht umgesetzt.

IT-Grundschutz-Check - Dokumentation

SerNet

- Nummer, Bezeichnung und Standort der/des Zielobjekte/s
- Der modellierte Baustein
- Erfassungsdatum und Name des Erfassers
- Befragte Ansprechpartner
- Umsetzungsstatus (entbehrlich/ja/teilweise/nein)
- Umsetzung bis
- Verantwortliche
- Bemerkungen / Begründungen
- Defizite / Kostenschätzung

=> Report A.4 IT-Grundschutz-Check

Risikoanalyse

SerNet

Risikobewertung implizit für Bereiche mit normalem Schutzbedarf

(Gefährdungen, die eine so hohe Eintrittswahrscheinlichkeit oder so einschneidende Auswirkungen haben, dass Sicherheitsmaßnahmen ergriffen werden müssen)

Explizite Risikoanalyse muss durchgeführt werden, wenn der Informationsverbund Zielobjekte enthält, die:

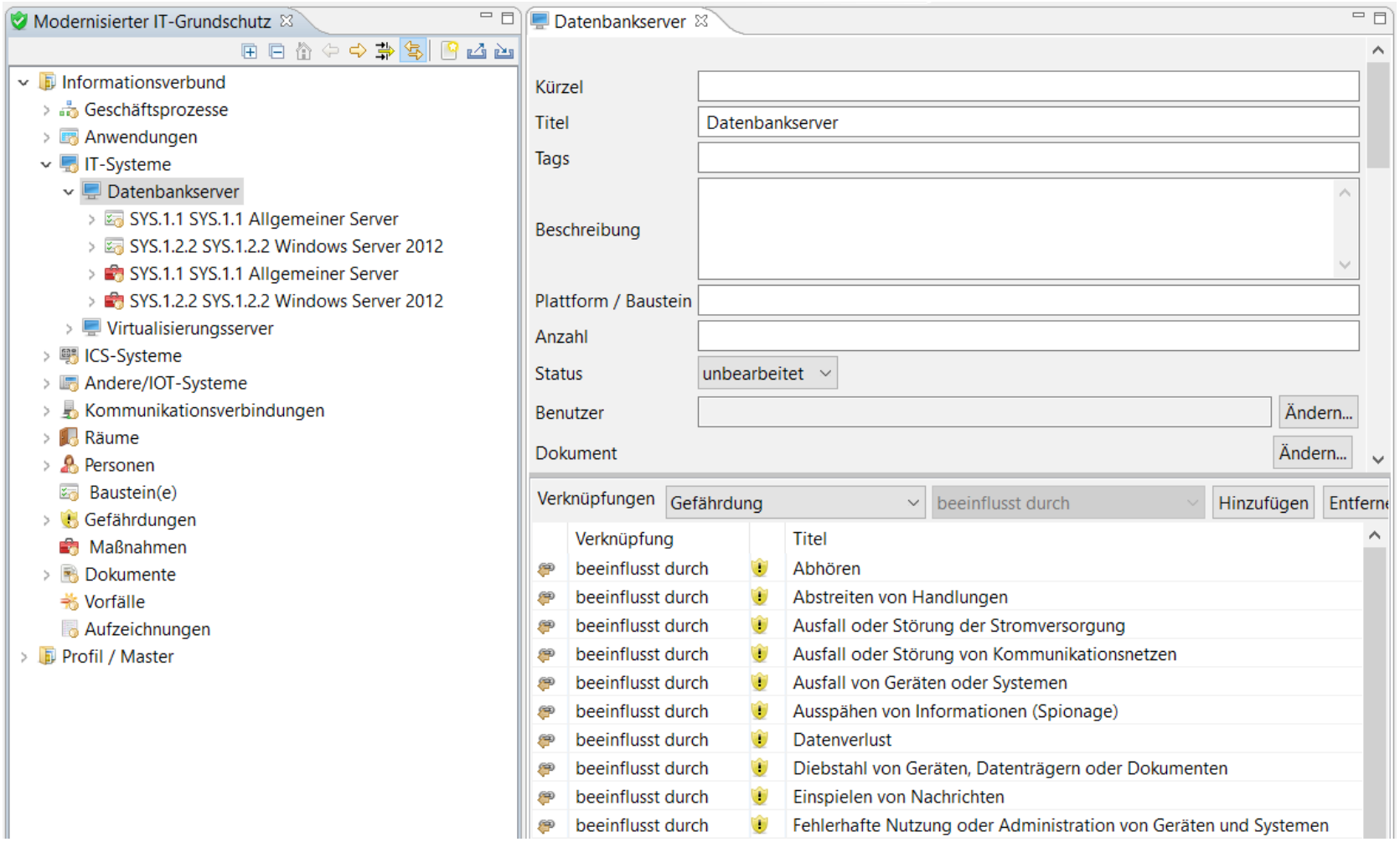
- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend modelliert werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT- Grundschutzes nicht vorgesehen sind.

In diesen Fällen stellen sich folgende Fragen:

- Welchen Gefährdungen für die Informationsverarbeitung ist durch die Umsetzung der relevanten IT-Grundschutz-Bausteine noch nicht ausreichend oder sogar noch gar nicht Rechnung getragen?
- Müssen eventuell ergänzende Sicherheitsmaßnahmen, die über das IT-Grundschutz-Modell hinausgehen, eingeplant und umgesetzt werden?

Risikoanalyse - Gefährdungsübersicht

SerNet



Risikoanalyse - Risikoeinstufung

SerNet

	Datenbankserver: Vertraulichkeit: hoch Integrität: hoch Verfügbarkeit: hoch			Eintrittswahrscheinlichkeit ohne zusätzliche Maßnahmen: selten mittel häufig sehr häufig	Auswirkung ohne zusätzliche Maßnahmen: vernachlässigbar begrenzt beträchtlich existenzbedrohend	Risiko ohne zusätzliche Maßnahmen: gering mittel hoch sehr hoch	Risikobehandlung: Reduzieren (Modifizieren) Vermeiden Transferieren Übernehmen Akzeptieren
	Verknüpfung		**Titel**	**Eintrittswahrscheinlichkeit**	**Auswirkung**	**Risiko**	**Risikobehandlung**
	beeinflusst durch		G 0.15 Abhören	selten	vernachlässigbar	gering	Akzeptieren
	beeinflusst durch		G 0.27 Ressourcenmangel	selten	begrenzt	gering	Akzeptieren
	beeinflusst durch		G 0.33 Personalausfall	mittel	beträchtlich	mittel	Übernehmen
	beeinflusst durch		G 0.36 Identitätsdiebstahl	häufig	existenzbedrohend	sehr hoch	Vermeiden
	beeinflusst durch		G 0.39 Schadprogramme	selten	vernachlässigbar	gering	Akzeptieren
	beeinflusst durch		G 0.41 Sabotage	sehr häufig	begrenzt	hoch	Vermeiden
	beeinflusst durch		G 0.43 Einspielen von Nachrichten	häufig	beträchtlich	hoch	Transferieren
	beeinflusst durch		Z 1.1 Zusätzliche Gefährdung	sehr häufig	existenzbedrohend	sehr hoch	Vermeiden

Vielen Dank!