

Der Modernisierte Grundschutz in verinice

verinice.XP 2018

Michael Flürenbrock

verinice Product Owner

---

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

# Strukturanalyse - Prozesse

The screenshot displays the SerNet software interface. On the left, a tree view shows the organizational structure under 'Modernisierter IT-Grundschutz'. The tree is expanded to show 'Geschäftsprozesse' (Business Processes), which includes 'a Kernprozesse' (Core Processes) and 'b Fachaufgaben' (Specialized Tasks). Under 'a Kernprozesse', 'Geschäftsprozess 1' is selected. Under 'b Fachaufgaben', 'Fachaufgabe 1' and 'Fachaufgabe 2' are listed. Below the tree, a list of applications is shown, including 'Application Gateway', 'Auftrags- und Kundenverwaltung', 'Benutzerauthentisierung', 'Druckservice Bad Godesberg', 'Druckservice Beuel', 'E-Mail, Terminkalender', 'Faxen', 'Finanzbuchhaltung', 'Internet-Recherche', 'Office-Anwendungen', 'Personaldatenverarbeitung', 'Reisekostenabrechnung', and 'Systemmanagement'.

The right pane shows the configuration for 'Geschäftsprozess 1'. The fields are as follows:

- Kürzel: [Empty text box]
- Titel: Geschäftsprozess 1
- Beschreibung: [Empty text area]
- Tags: [Empty text box]
- Prozess-Art: unbearbeitet (dropdown menu)
- Mitarbeiter: [Empty text box] with an 'Ändern...' button
- Dokument: [Empty text box] with an 'Ändern...' button
- ▼ Schutzbedarf
  - Vertraulichkeit ableiten nach Maximumprinzip:
  - Vertraulichkeit nach Verteilung/Kumulationseffekt: Unbearbeitet (dropdown menu)
  - Vertraulichkeit: Unbearbeitet (dropdown menu)
  - Begründung Vertraulichkeit: [Empty text area]

# Strukturanalyse Zielobjekte

The screenshot displays the SerNet software interface. On the left, a tree view shows the hierarchy of IT assets under 'Modernisierter IT-Grundschutz'. The 'Räume' (Rooms) folder is expanded, showing 'Serverraum 1' selected. On the right, the 'Serverraum 1' form is open, showing fields for 'Kürzel', 'Titel', 'Beschreibung', 'Plattform / Baustein', 'Anzahl', 'Status', 'Tags', 'Benutzer', and 'Dokument'. The 'Status' is set to 'unbearbeitet'. Below the form is a 'Verknüpfungen' (Links) table.

| Verknüpfung      | Titel      | Scope               | Beschreibung |
|------------------|------------|---------------------|--------------|
| beinhaltet       | Server 1   | Informationsverbund |              |
| Verantwortlicher | Tech, Nick | Informationsverbund |              |
| befindet sich in | Altbau     | Informationsverbund |              |

# Schutzbedarfsfeststellung & -vererbung

Geschäftsprozess 1 Office-Anwendungen

Kürzel

Titel Geschäftsprozess 1

Beschreibung

Tags

Prozess-Art Kerngeschäft

Mitarbeiter

Dokument

▼ Schutzbedarf

Vertraulichkeit ableiten nach Maximumprinzip

Vertraulichkeit nach Verteilung/Kumulationseffekt Unbearbeitet

Vertraulichkeit Normal

Begründung Vertraulichkeit

Integrität ableiten nach Maximumprinzip

Integrität nach Verteilung/Kumulationseffekt Unbearbeitet

Integrität Normal

Begründung Integrität

Verfügbarkeit ableiten nach Maximumprinzip

Verfügbarkeit nach Verteilung/Kumulationseffekt Unbearbeitet

Verfügbarkeit Normal

Begründung Verfügbarkeit

Office-Anwendungen

Kürzel

Titel Office-Anwendungen

Tags

Beschreibung

Plattform / Baustein

Anzahl

Status unbearbeitet

Benutzer

Dokument

▼ Schutzbedarf

Vertraulichkeit ableiten nach Maximumprinzip

Vertraulichkeit nach Verteilung/Kumulationseffekt Unbearbeitet

Vertraulichkeit Normal

Begründung Vertraulichkeit

Integrität ableiten nach Maximumprinzip

Integrität nach Verteilung/Kumulationseffekt Kumulationseffekt

Integrität Hoch

Begründung Integrität

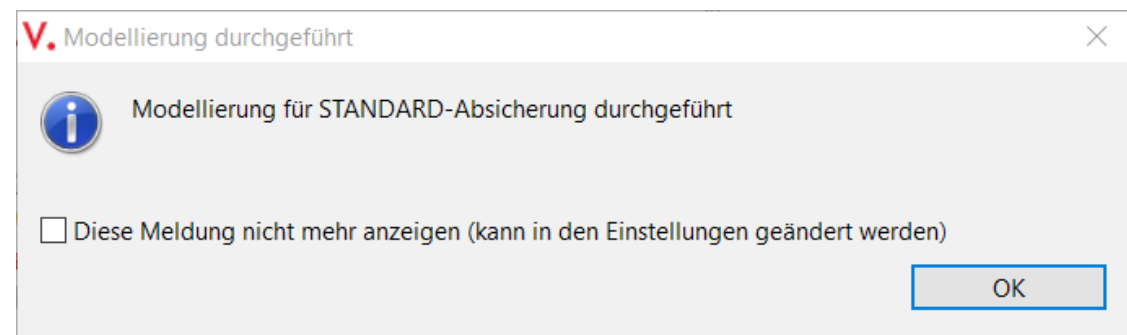
Verknüpfungen

| Verknüpfung | Titel              | Scope               | Beschreibung |
|-------------|--------------------|---------------------|--------------|
| nötig für   | Geschäftsprozess 1 | Informationsverbund |              |

# Modellierung – Vorgehensweise der Absicherung

Informationsverbund ✕

|                                |                     |
|--------------------------------|---------------------|
| Titel                          | Informationsverbund |
| Abkürzung                      |                     |
| Tags                           |                     |
| Anzahl Mitarbeiter             |                     |
| Geltungsbereich                |                     |
| Vorgehensweise der Absicherung | STANDARD ▾          |



# Modellierung – Anforderungen & Maßnahmen

The screenshot displays the SerNet software interface, which is used for modeling requirements and measures. It is divided into several main sections:

- Benutzervorgaben (User Settings):** A sidebar on the left containing various configuration options such as 'Installieren/Aktualisieren', 'Allgemeine Einstellungen', 'BSI IT-Grundschutz', 'Betriebsmodus', 'Datenbank', 'GSTOOL Import', 'Editor Einstellungen', 'Verschlüsselung', 'Hinweisdialoge', 'Standard Verzeichnisse', 'Suche', 'VNA Import / Export', 'Datei-Objekt-Import', 'Active Directory', 'Reports', 'Security Assessment Einstellungen', and 'Netzwerkverbindungen'.
- BSI IT-Grundschutz (BSI IT Basic Protection):** A central window for configuring the data source for the BSI protection catalog. It includes instructions on how to download the catalog and a text field for the ZIP file path: 'Z:\VMwareHost(Content)\IT-Grundschutzkataloge\it-grundschutz\_el15\_verinice.zip'. A checkbox labeled 'Modelliere Umsetzungshinweise / Maßnahmen' (Model implementation instructions / measures) is checked and highlighted with a red box.
- Modernisierter IT-Grundschutz (Modernized IT Basic Protection):** A tree view on the left showing a hierarchical structure of IT systems. The 'Virtualisierungsserver' (Virtualization server) is selected, showing sub-items like 'SYS.1.1 SYS.1.1 Allgemeiner Server', 'SYS.1.2.2 SYS.1.2.2 Windows Server 2012', and 'Maßnahmen' (Measures).
- Virtualisierungsserv (Virtualization Server):** A configuration window on the right for the selected server. It includes fields for 'Kürzel' (Alias), 'Titel' (Title: 'Virtualisierungsserver'), 'Tags', 'Beschreibung', 'Plattform / Baustein' (Platform / Component), 'Anzahl' (Quantity), and 'Status' (Status: 'Betrieb'). Below these fields is a table of 'Verknüpfungen' (Links) connecting the server to various security measures.

| Verknüpfung       | Titel  |
|-------------------|--|
| Verantwortlicher  | Ad, Min  |
| befindet sich in  | Serverraum 1   |
| modelliert mit    | Sichere Administration von Windows Server 2012                     |
| modelliert mit    | Sichere Authentisierung und Autorisierung in Windows Server 2012   |
| modelliert mit    | Sichere Installation und Grundkonfiguration von Servern            |
| modelliert mit    | Systemüberwachung  |
| modelliert mit    | Unterbrechungsfreie und stabile Stromversorgung                    |
| modelliert mit    | Updates und Patches für Firmware, Betriebssystem und Anwendungen   |
| modelliert mit    | Verschlüsselung der Kommunikationsverbindungen                     |
| beeinflusst durch | Social Engineering   |
| beeinflusst durch | Software-Schwachstellen oder -Fehler                               |
| beeinflusst durch | Unbefugtes Eindringen in IT-Systeme                                |
| beeinflusst durch | Unbefugtes Eindringen in Räumlichkeiten                            |
| beeinflusst durch | Unberechtigte Nutzung oder Administration von Geräten und Systemen |
| beeinflusst durch | Verhinderung von Diensten (Denial of Service)                      |
| beeinflusst durch | Verstoß gegen Gesetze oder Regelungen                              |

# Modellierung - Umsetzungsstatus

The screenshot displays a software interface for IT system modeling. On the left, a tree view shows the hierarchy of systems under 'Modernisierter IT-Grundschatz'. The selected item is 'SYS.1.1.A1 [BASIS] Geeignete Aufstellung'. The right pane shows the configuration details for this system.

**Tree View (Left):**

- Informationsverbund
  - Geschäftsprozesse
  - Anwendungen
  - IT-Systeme
    - Datenbankserver
      - SYS.1.1 SYS.1.1 Allgemeiner Server
        - SYS.1.1.A1 [BASIS] Geeignete Aufstellung**
        - SYS.1.1.A2 [BASIS] Benutzerauthentisierung
        - SYS.1.1.A3 [BASIS] Restriktive Rechtevergabe
        - SYS.1.1.A4 [BASIS] Rollentrennung
        - SYS.1.1.A5 [BASIS] Schutz der Administrationsschnittstellen
        - SYS.1.1.A6 [BASIS] Deaktivierung nicht benötigter Dienste und
        - SYS.1.1.A7 [BASIS] Updates und Patches für Firmware, Betriebs
        - SYS.1.1.A8 [BASIS] Regelmäßige Datensicherung
        - SYS.1.1.A9 [BASIS] Einsatz von Viren-Schutzprogrammen
        - SYS.1.1.A10 [BASIS] Protokollierung
        - SYS.1.1.A11 [STANDARD] Festlegung einer Sicherheitsrichtlinie
        - SYS.1.1.A12 [STANDARD] Planung des Server-Einsatzes
        - SYS.1.1.A13 [STANDARD] Beschaffung von Servern
        - SYS.1.1.A14 [STANDARD] Erstellung eines Benutzer- und Admin
        - SYS.1.1.A15 [STANDARD] Unterbrechungsfreie und stabile Stro
        - SYS.1.1.A16 [STANDARD] Sichere Installation und Grundkonfigu
        - SYS.1.1.A17 [STANDARD] Einsatzfreigabe
        - SYS.1.1.A18 [STANDARD] Verschlüsselung der Kommunikations
        - SYS.1.1.A19 [STANDARD] Einrichtung lokaler Paketfilter
        - SYS.1.1.A20 [STANDARD] Beschränkung des Zugangs über Net
        - SYS.1.1.A21 [STANDARD] Betriebsdokumentation
        - SYS.1.1.A22 [STANDARD] Einbindung in die Notfallplanung
        - SYS.1.1.A23 [STANDARD] Systemüberwachung
        - SYS.1.1.A24 [STANDARD] Sicherheitsprüfungen
        - SYS.1.1.A25 [STANDARD] Regelmäßige Außerbetriebnahme eines
        - SYS.1.1.A26 [ERHÖHT] Mehr-Faktor-Authentisierung
        - SYS.1.1.A27 [ERHÖHT] Hostbasierte Angriffserkennung
        - SYS.1.1.A28 [ERHÖHT] Redundanz
        - SYS.1.1.A29 [ERHÖHT] Einrichtung einer Testumgebung

**Configuration View (Right):**

**Geeignete Aufstellung**

- Identifizier: SYS.1.1.A1
- Titel: Geeignete Aufstellung
- Vorgehensweise: BASIS
- Beschreibung: [Empty text area]
- Tags: [Empty text area]
- Dokument: [Ändern...](#)
- Letzte Änderung: 14.09.2017
- Vertraulichkeit:
- Integrität:
- Verfügbarkeit:
- Umsetzung
  - Umsetzungsstatus aus Maßnahme ableiten:
  - Umsetzungsstatus: Ja
  - Erläuterung: [Empty text area]
- Revision: [Empty text area]
- Datenschutzziele nach Art. 32 EU-DSGVO: [Empty text area]
- KIX: [Empty text area]

**Verknüpfungen:**

| Verknüpfung     | Titel                  | Scope         | Beschreibung |
|-----------------|------------------------|---------------|--------------|
| modelliert      | Datenbankserver        | Informatio... |              |
| reduziert Ei... | Ausfall oder Störun... | Informatio... |              |
| reduziert Ei... | Ausfall oder Störun... | Informatio... |              |



# Modellierung – Umsetzungsstatus ableiten








The screenshot displays the SerNet interface. On the left, a tree view under 'Modernisierter IT-Grundschutz' shows a hierarchy of IT systems. The selected item is 'SYS.1.1.A1 [BASIS] Geeignete Aufstellung'. The main panel on the right shows the configuration for this system.

**Identifizierung:** Identifizier: SYS.1.1.A1, Titel: Geeignete Aufstellung, Vorgehensweise: BASIS

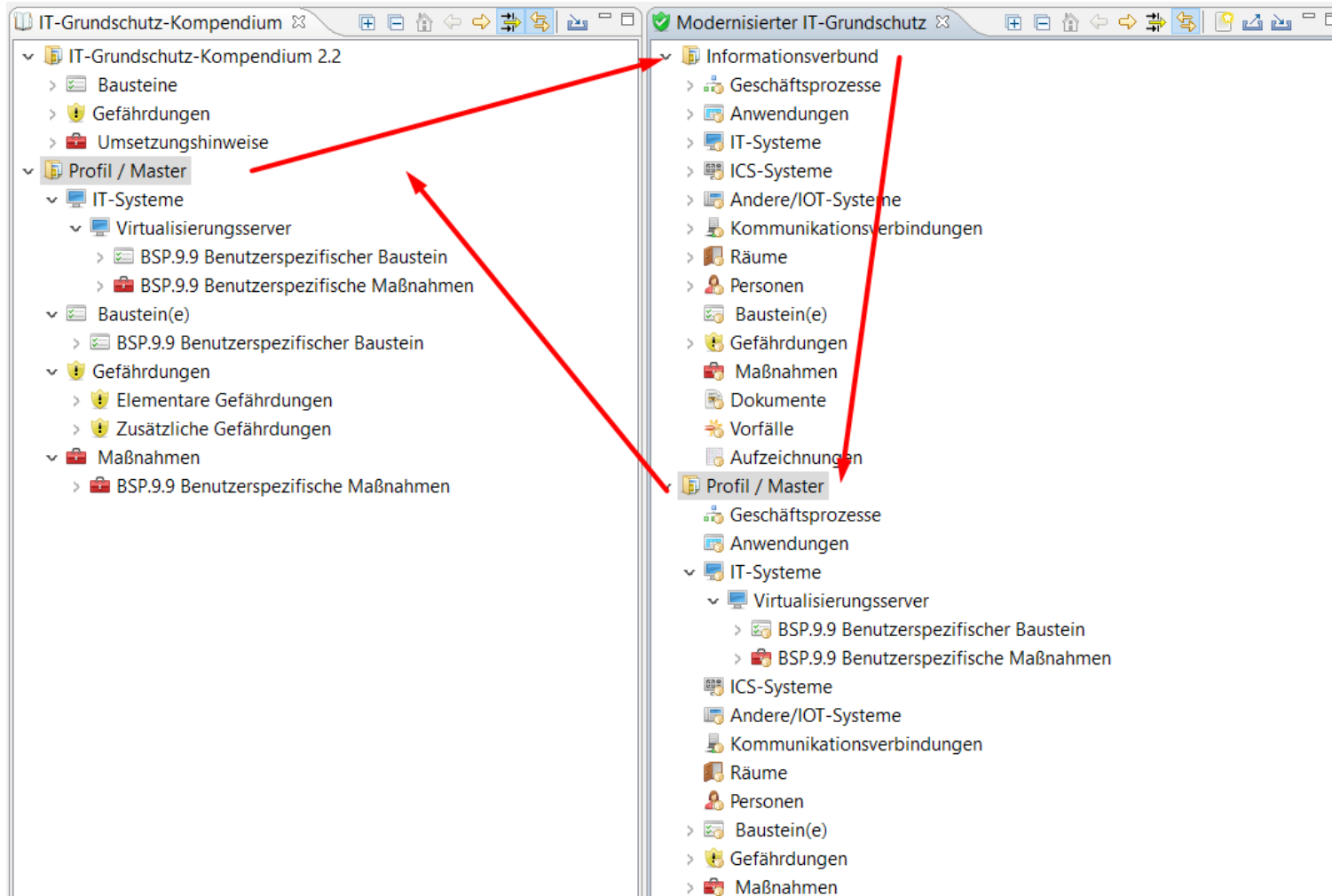
**Umsetzung:** Umsetzungsstatus aus Maßnahme ableiten:  Umsetzungsstatus: Ja

**Verknüpfungen:**

| Verknüpfung                               | Titel   |
|---|---|
| erfüllt durch                             | Geeignete Aufstellung                         |
| reduziert Eintrittswahrscheinlichkeit von | Ausfall oder Störung der Stromversorgung      |
| reduziert Eintrittswahrscheinlichkeit von | Ausfall oder Störung von Kommunikationsnetzen |
| reduziert Eintrittswahrscheinlichkeit von | Ausfall von Geräten oder Systemen             |

- ▼  Baustein(e)
  - ▼  BSP.9.9 Benutzerspezifischer Baustein
    - ❗ BSP.9.9.A1 [] Benutzerspezifische Anforderung 1
    - ❗ BSP.9.9.A2 [BASIS] Benutzerspezifische Anforderung 2
    - ❗ BSP.9.9.A3 [STANDARD] Benutzerspezifische Anforderung 3
    - ❗ BSP.9.9.A4 [ERHÖHT] Benutzerspezifische Anforderung 4
- ▼  Gefährdungen
  - >  Elementare Gefährdungen
  - ▼  Zusätzliche Gefährdungen
    - ⚠ Z A.1 Zusätzliche Gefährdung A
    - ⚠ Z B.1 Zusätzliche Gefährdung B
- ▼  Maßnahmen
  - ▼  BSP.9.9 Benutzerspezifische Maßnahmen
    - ❗ BSP.9.9.M1 [] Benutzerspezifische Maßnahmen 1
    - ❗ BSP.9.9.M2 [BASIS] Benutzerspezifische Maßnahmen 2
    - ❗ BSP.9.9.M3 [STANDARD] Benutzerspezifische Maßnahmen 3
    - ❗ BSP.9.9.M4 [ERHÖHT] Benutzerspezifische Maßnahmen 4

# Modellierung – Profile / Templates



The screenshot shows the 'Modernisierter IT-Grundschutz' application. The left pane displays a tree view of IT systems, with 'SYS.1.1 Allgemeiner Server' selected. The right pane shows a table of requirements and their responsible parties.

| 3 Anforderungen         |             |
|-------------------------|-------------|
| Hauptverantwortlicher   | IT-Betrieb  |
| Weitere Verantwortliche | Haustechnik |

**3.1 Basis-Anforderungen**

Die folgenden Anforderungen MÜSSEN vorrangig umgesetzt werden:

**SYS.1.1.A1 Geeignete Aufstellung [Haustechnik]**

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server MÜSSEN daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden, siehe hierzu die entsprechenden Bausteine. Es MUSS geregelt werden, wer Zutritt zu den Räumen beziehungsweise physischen Zugang auf die Server selbst erhält. Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden.

Es MUSS auf eine geeignete räumliche Trennung der Systeme, die gesichert werden sollen, von den sichernden Systemen, etwa Backup-Servern in unterschiedlichen Brandabschnitten, geachtet werden, um die Auswirkungen bei einem physischen Schaden zu begrenzen.

**SYS.1.1.A2 Benutzerauthentisierung**

Um den Server zu nutzen, MÜSSEN sich die Benutzer gegenüber dem IT-System authentisieren. Sollen hierfür die Benutzer und Administratoren Passwörter verwenden, MÜSSEN sichere Passwörter benutzt werden. Hierfür SOLLTE es eine Passwort-Richtlinie geben.

- Dokumentation sichten
- Externe Stellen identifizieren
- Hauptansprechpartner identifizieren

„... 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**.

- 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

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















The screenshot displays the SerNet software interface. On the left, a tree view shows the project structure under 'Modernisierter IT-Grundschatz', with 'Datenbankserver' selected. The main window shows the details for the 'Datenbankserver' asset, including fields for 'Kürzel', 'Titel', 'Tags', 'Beschreibung', 'Plattform / Baustein', 'Anzahl', 'Status' (set to 'unbearbeitet'), and 'Benutzer'. Below these fields is a 'Verknüpfungen' table showing a list of threats that influence the asset.

| Verknüpfung       | Gefährdung   | beeinflusst durch | Hinzufügen | Entfernen |
|-------------------|--|-------------------|------------|-----------|
| beeinflusst durch | Abhören  |                   |            |           |
| beeinflusst durch | Abstreiten von Handlungen  |                   |            |           |
| beeinflusst durch | Ausfall oder Störung der Stromversorgung                         |                   |            |           |
| beeinflusst durch | Ausfall oder Störung von Kommunikationsnetzen                    |                   |            |           |
| beeinflusst durch | Ausfall von Geräten oder Systemen                                |                   |            |           |
| beeinflusst durch | Ausspähen von Informationen (Spionage)                           |                   |            |           |
| beeinflusst durch | Datenverlust   |                   |            |           |
| beeinflusst durch | Diebstahl von Geräten, Datenträgern oder Dokumenten              |                   |            |           |
| beeinflusst durch | Einspielen von Nachrichten                                       |                   |            |           |
| beeinflusst durch | Fehlerhafte Nutzung oder Administration von Geräten und Systemen |                   |            |           |



# Risikoanalyse - Risikoeinstufung

|                       |  |  |   |                                       |  |
|-----------------------|--|--|---|---------------------------------------|--|
| Datenbankservers:     |  | Eintrittswahrscheinlichkeit<br>ohne zusätzliche Maßnahmen: | Auswirkung<br>ohne zusätzliche Maßnahmen: | Risiko<br>ohne zusätzliche Maßnahmen: | Risikobehandlung:<br>Reduzieren (Modifizieren) |
| Vertraulichkeit: hoch |  | selten   | vernachlässigbar                          | gering                                | Vermeiden                                      |
| Integrität: hoch      |  | mittel   | begrenzt                                  | mittel                                | Transferieren                                  |
| Verfügbarkeit: hoch   |  | häufig   | beträchtlich                              | hoch                                  | Übernehmen                                     |
|                       |  | sehr häufig  | existenzbedrohend                         | sehr hoch                             | 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!

---