Grundschutz mit Verinice

Zweck: Modellierung gemäß BSI Std. 100-2, Kap. 4

Vorbereitung u.a.:
Netzplan (Std. Seite 45) erstellen,
verwandte Geräte sinnvoll gruppieren / zusammenfassen!

Starten, Tab "IT Grundschutz"
Beim 1. Mal: Bearbeiten/Einstellungen, BSI IT Grundschutz: **Kataloge laden**

Grundsätzliches Vorgehen:

1.) Systeme usw. anlegen ("Hirn" gefragt)
2.) Bausteine zuordnen (aus dem Grundschutz-Katalog)
3.) Verknüpfungen definieren ("Hirn" gefragt)
4.) Schutzbedarf festlegen (BSI Std. 100-2, Kap. 4.3)
5.) Maßnahmen durchgehen (BSI Std. 100-2, Kap. 4.4 / 4.5)

Ad 1.:
"Anwendungen", "IT-Systeme: ...", "Räume", ...
Rechtsklick im Tree auf "Anwendungen", "IT-Systeme", ..., Menüpunkt "Neue ..." wählen
Doppelklick im Tree: Rechts werden Detaildaten angezeigt ==› Ausfüllen!
"Personen": Laut BSI-Std. nicht für Modellierung nötig
    Aber: Zuordnung von Aufgaben & Verantwortlichkeiten
    ==› verinice generiert Arbeitspläne!

Ad 2.:
Bausteine von Baustein-Katalog ganz links auf die Objekte im Tree ziehen
==› Bei den Objekten werden automatisch Maßnahmen eingetragen!
Grundlage: Dokument "Grundschutz-Katalog", Kap. 2.2:
"Zuordnung anhand Schichtenmodell"
==› Legt **verpflichtende** Bausteine fest!!!
==› Katalog Liste "Übergreifende Aspekte ...":
Einige Bausteine (19 Bausteine B1.x) gelten modellweit:
    Oben auf die Wurzel "IT Netzwerk" ziehen!
    Vereinfachung: Rechtsklick auf Tree-Objekt, "Bausteine automatisch zuordnen"

Ad 3.:
"Anwendung läuft auf Server", "Server steht in Raum", ...
Mittels Drag & Drop erstellen:
Automatische Einträge "nötig für", "beinhaltet", "befindet sich in", "benötigt", ...
in Verknüpfungs-Tabelle (am unteren Ende der Detaildaten-Ansicht)
Doppelklick auf Zeile der Verknüpfungs-Tabelle sprint zum Zielobjekt!
Die Kauf-Version kann eine Zuordnungs-Tabelle als Report erzeugen

Ad 4.:
Schutzbedarf wird zuerst bei den *Anwendungen* festgelegt:
Doppelklick, runterscrollen, Level gemäß BSI-Std. wählen
==› Verinice vererbt sie auf Server, Raum, …
Dazu bei Server usw. im Feld "Begründung Vertraulichkeit" usw. auswählen
(schaut aus wie ein Textfeld, ist aber ein Pulldown mit Cursor-runter-Taste):
"Maximalprinzip":
Level wird automatisch höchstes Level der zugeordneten Objekte, nicht änderbar
"Kumulationseffekt":
Dasselbe, aber kann händisch höher festgelegt werden:
Viele kleine Schutzbedürfnisse summieren sich zu einem größeren
("viele wichtige Anwendungen ==› Server ist sogar sehr wichtig")
"Verteilungseffekt":
Dasselbe, aber kann händisch niedriger festgelegt werden :
Schutzbedarf verteilt sich auf mehrere redundante Server, Standorte, …
("Anwendung ist auf viele Server im Cluster verteilt ==› ein paar dürfen ausfallen")
Ad 5.:
Doppelklick auf die Maßnahme, zu "Umsetzung" scrollen:
"Ja": Maßnahme ist komplett erledigt
"Entbehrlich": Gefahr ist nicht vorhanden / nicht relevant
"Teilweise": Umsetzung der Maßnahme ist fix geplant bzw. schon in Arbeit
==› Datum & Mitarbeiter eingeben
==› Verinice generiert daraus Arbeitspläne!
"Nein": "Wir wollen das machen, aber haben noch nichts gemacht"
In Real: Entscheidung und Umsetzung in weiteren Feldern dokumentieren!
Wenn alle Maßnahmen erledigt sind:
Das erreichte Schutzniveau wird beim Baustein-Icon eingeblendet:
Level A, B, C, Z (A-C Pflicht für Grundschutz, Z Option für hohen Schutzbedarf)
Vorbereitung ev. "alle aufklappen"
Schnell-Erledigung ev. Multi-Select, Rechtsklick "Masseneditor"

Ergänzende Sicherheits-Analyse:

- BSI Std 100-3
- Kurzanleitung BSI Std 100-2 Kap 4.6 "Ergänzende Sicherheits-Analyse"

Siehe Kap 4.6.2:

0. Schritt: Ergänzende Sicherheits-Analyse überhaupt nötig?

Schutzbedarf "normal" & "keine besonderen Umstände"
==› Mit normaler Abhandlung des Grundschutzes alles erledigt

- Entweder: Schutzbedarf "hoch" oder "sehr hoch"

- Oder: "Besondere Umstände" führen zu Risiken,
  die nicht durch Standard-Risiko-Bausteine abgedeckt sind

==> Ergänzende Sicherheits-Analyse machen!

Bsp.: Linux-Laptop in Außeneinsatz Panzer (z.B. für Navigationsaufgaben)
==> Std-Bausteine "Allg. Client", "Client unter Linux", "Laptop"
==> Alles nur für Büro & normaler Mobil-Einsatz
(auch keine passenden Arbeitsplatz-Standardbausteine unter "Infrastruktur")
==> Hitze, Erschütterung, spezielle Stromversorgung usw. nicht abgedeckt!

1. Schritt: "Decken die bestehenden Maßnahmen die Risiken?"

Ja ==> Nichts weiter tun
Nein ==> Risiko-Analyse nötig

In verinice: "Management-Bewertung"
a) Warum?
(siehe oben 0. Schritt:
Wegen "hoch"/"sehr hoch" oder wegen besonderer Umstände?)
b) Risiko-Analyse nötig? (siehe oben: "Decken die bestehenden Maßnahmen die Risiken?")
c) Begründung, vor allem wenn "nicht nötig"
==> Verantwortlichen für die Entscheidung dokumentieren

2. Schritt: Siehe 100-2 Kap 4.6.3

a) Welche Gefährdungen sind zu beachten?
b) Check Gefährdungen gegen betehende Mechanismen und Maßnahmen:
Sind die Mechanismen für die Gefährdungen
- Vollständig?
- Stark genug?
- Zuverlässig genug?
c) Wenn in b) Gefährdungen übrig bleiben:
Welche zusätzlichen Maßnahmen sind nötig?

In verinice:
Rechtsklick auf das Objekt ==> "Risiko-Analyse"
Öffnet Subfenster mit Liste aller Gefahren-Bausteine:

Ad a)
- Durch Standard-Bausteine behandelte Gefahren sind angehakt
- Ev. weitere Gefahren anhaken
- Ev. eigene Gefahren neu hinzufügen (Button [Neu]) und anhaken
Nummer üblicherweise bG1, bG2, ... ("b" für "benutzerdefiniert")

Ad b)
[Weiter] ==> Liste der ausgewählten Gefahren

Anhaken, was noch nicht abgedeckt ist

Ad c)
[Weiter] ==› Liste der noch offenen Gefahren
Letzte Spalte "Risiko-Alternative" bearbeiten
- "Reduktion":
    Ich setze eigene Maßnahmen, um die Gefahr zu reduzieren / eleminieren
- "Umstrukturierung":
    Ich baue meine Systemlandschaft so um, dass die Gefahr gar nicht auftreten kann
    (z.B. anderer Raum, anderer Server, anderes OS, ...)
- "Übernahme":
    "Ich lebe mit der Gefahr, trage sie selbst, wie sie ist"
- "Transfer":
    Ich verlagere das Risiko auf Externe
    (z.B. Outsourcing, Versicherung, ...)

Ad c), bei "Reduktion"
[Weiter]
    Maßnahmen von mittlerer Spalte auf Gefahren in linker Spalte ziehen
    Ev. auch neue Maßnahmen anlegen (Kürzel wieder bM1, ...)
[Fertigstellen]
==› Gefahren und Maßnahmen werden im Baum angezeigt
Weiter wie bisher: Doppelklick auf die Maßnahmen, rechts Umsetzung bearbeiten