verinice.XP

Modernisierter IT-Grundschutz

am Beispiel des Universitätsklinikums Halle (Saale)

Susanne Aust

27.02.2020

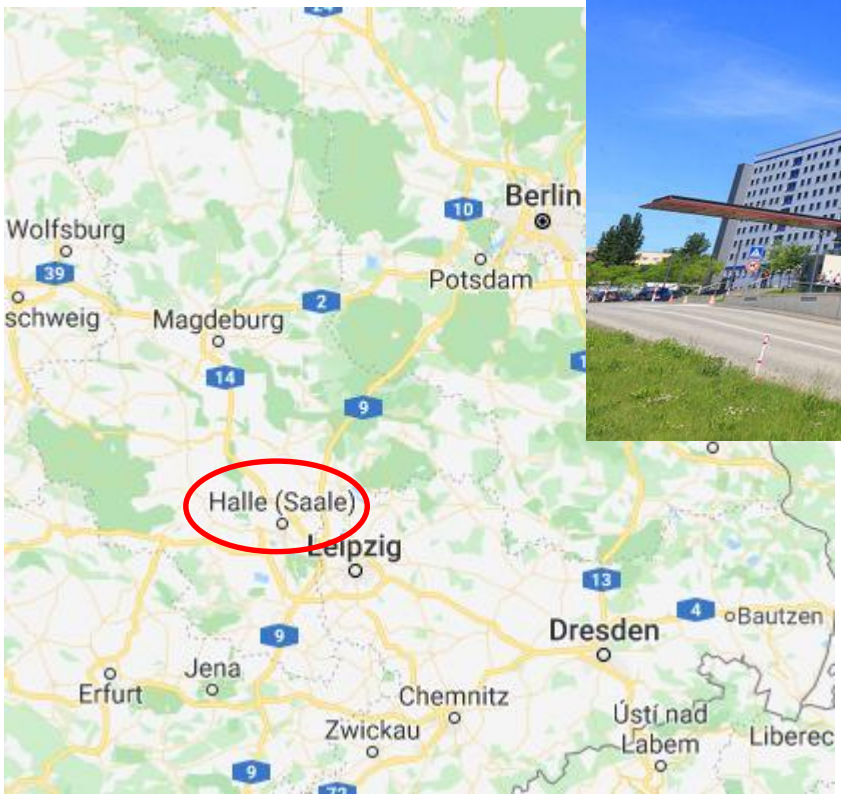
Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg

UKH
Universitätsklinikum
Halle (Saale)

Agenda

1. Vorstellung der Universitätsmedizin Halle (Saale)
2. Einführung eines ISMS nach BSI – Grundschutz
3. Vorgehensweise 2017 bis jetzt
    - Erfassung zentraler und dezentraler IT-Systeme
    - Einpflegen der Daten in Verinice
    - Modellierung nach modernisiertem BSI-Grundschutz
    - Dokumentation der Maßnahmen
    - Verteilen der Aufgaben
    - Prüfung nach §8a BSIG
    - Dokumentation von Vorfällen
4. Herausforderungen in Verinice

Halle (Saale):
ca. 240 000 Einwohner



UKH:
ca. 40.000 stationäre Fälle / Jahr

3 Standorte

Klinikum	Psychiatrie	Fakultät
		

10/2016: Bestellung des IT-Sicherheitsbeauftragten

Entscheidungen:

- BSI – Grundschutz
- IT – Sicherheit in der gesamten Universitätsmedizin (Klinikum + Fakultät)
- 04/2017: Koordinatorin für IT-Sicherheit im Rechenzentrum
- Pro Einrichtung ein/e IT-Beauftragte/r

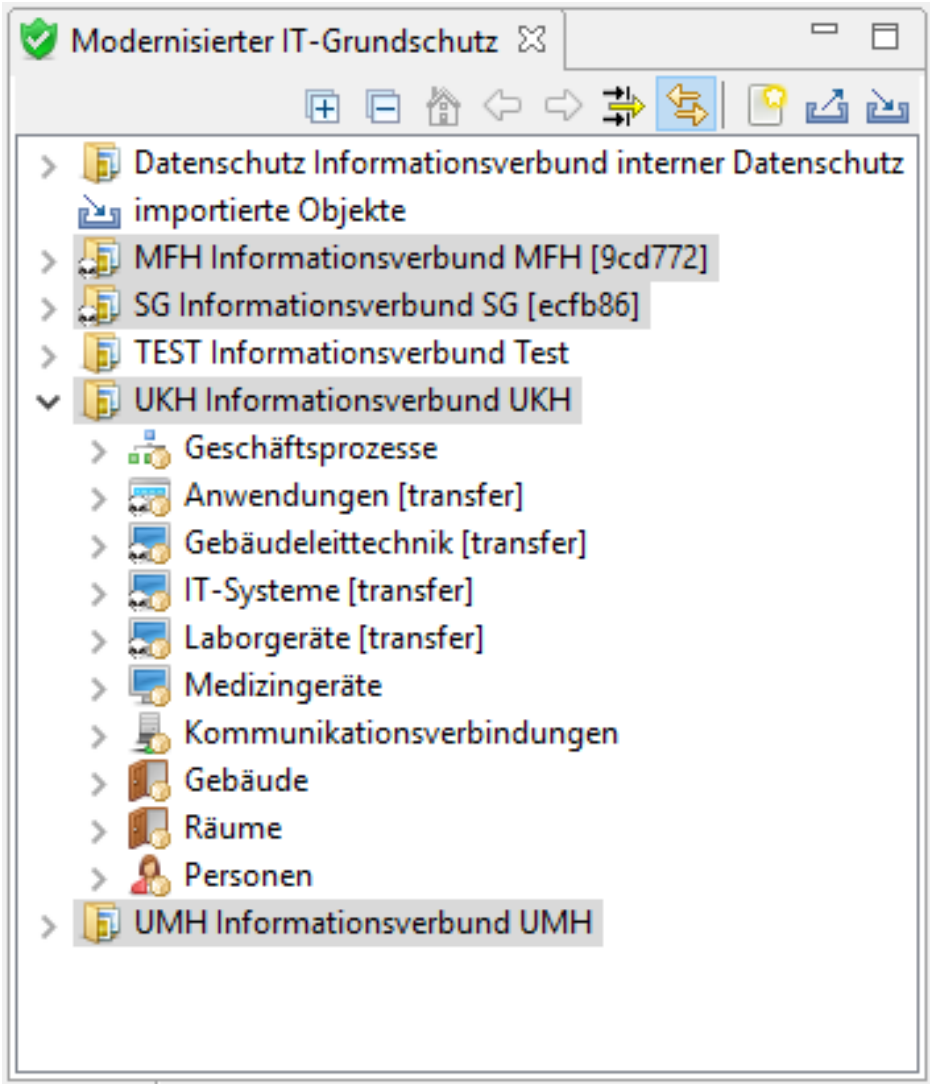

BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise
IT-Sicherheitsmanagement
Initiierung Sicherheitsprozess
IT-Sicherheitsleitlinie und -konzeption:
IT-Strukturanalyse
Schutzbedarfsfeststellung
Modellierung
Basis-Sicherheitscheck
Risikoanalyse
Realisierung
Aufrechterhaltung

Erfassung der zentralen und dezentralen IT – Systeme

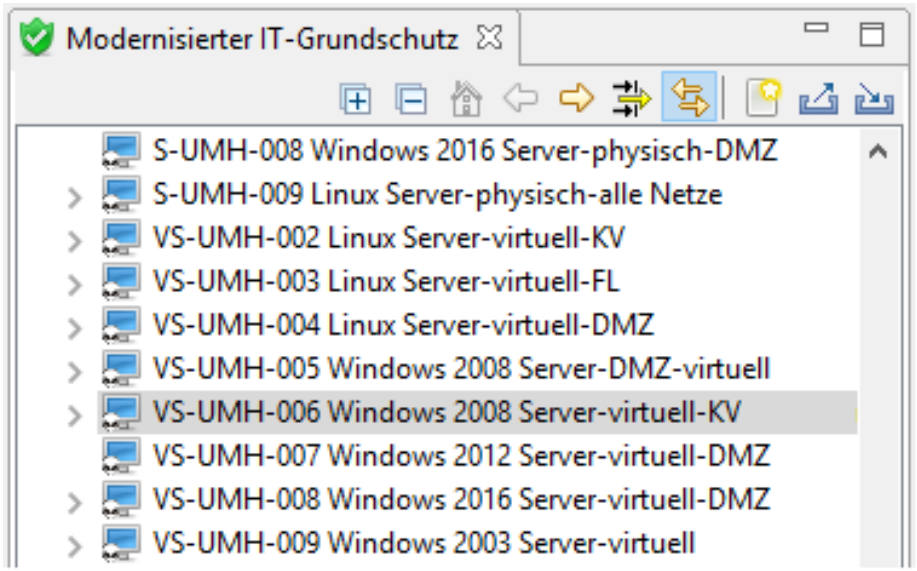
IT Systeme	Anzahl
Windows 7 Clients	2668
Windows 10 Clients	2255
Server	410
netzgebundene Medizin – und Laborgeräte	8776
Gebäudeleittechnik	7
Netzwerkkomponenten	278
WLAN-Access-Points	1106
Netzwerkdrucker	812
Drucker, MUFU, Scanner	1500
Anwendungen	891
Summe	**18.797**

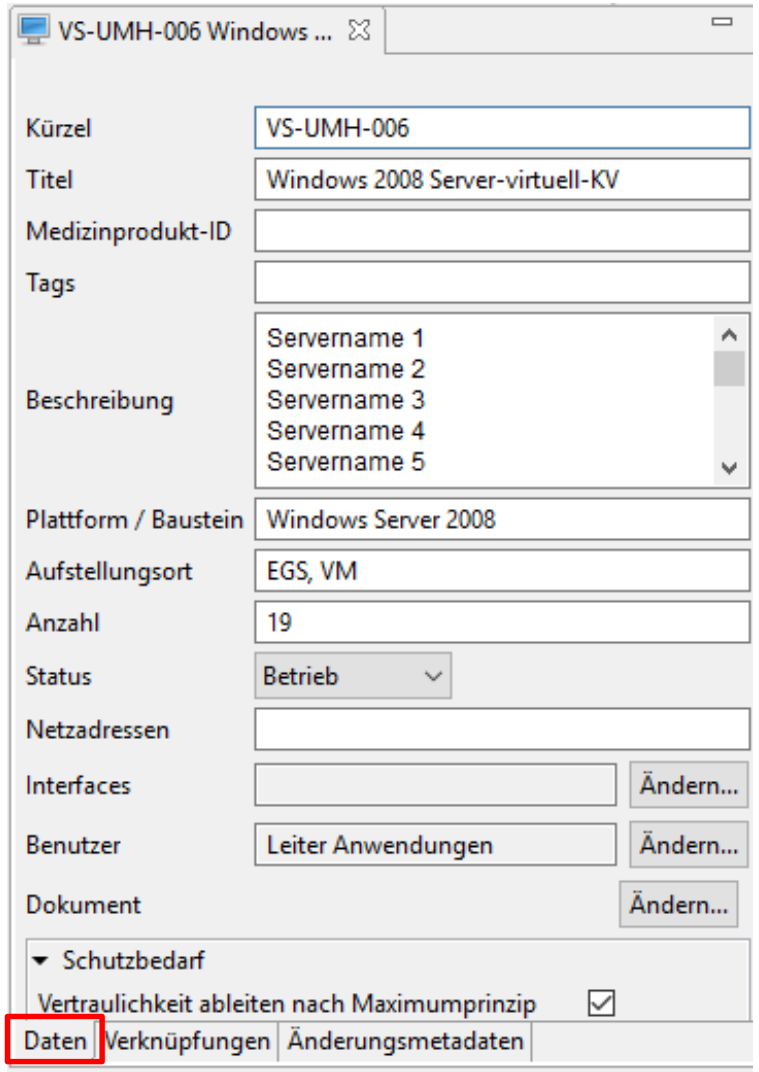
Unterstützung durch die Firma Sila Consulting

- 4 Informationsverbünde
  - Ein Übergeordneter
  - Drei Spezifische
- Unterteilung zusätzlicher IT-Systeme in:
  - Laborgeräte
  - Medizingeräte
  - Gebäudeleittechnik
- Medizingeräte werden größtenteils nicht in Verinice dokumentiert

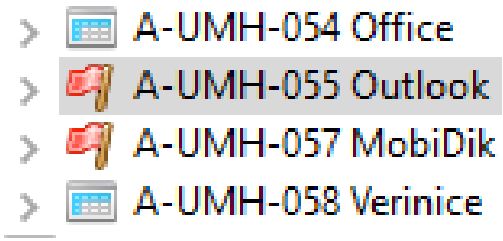


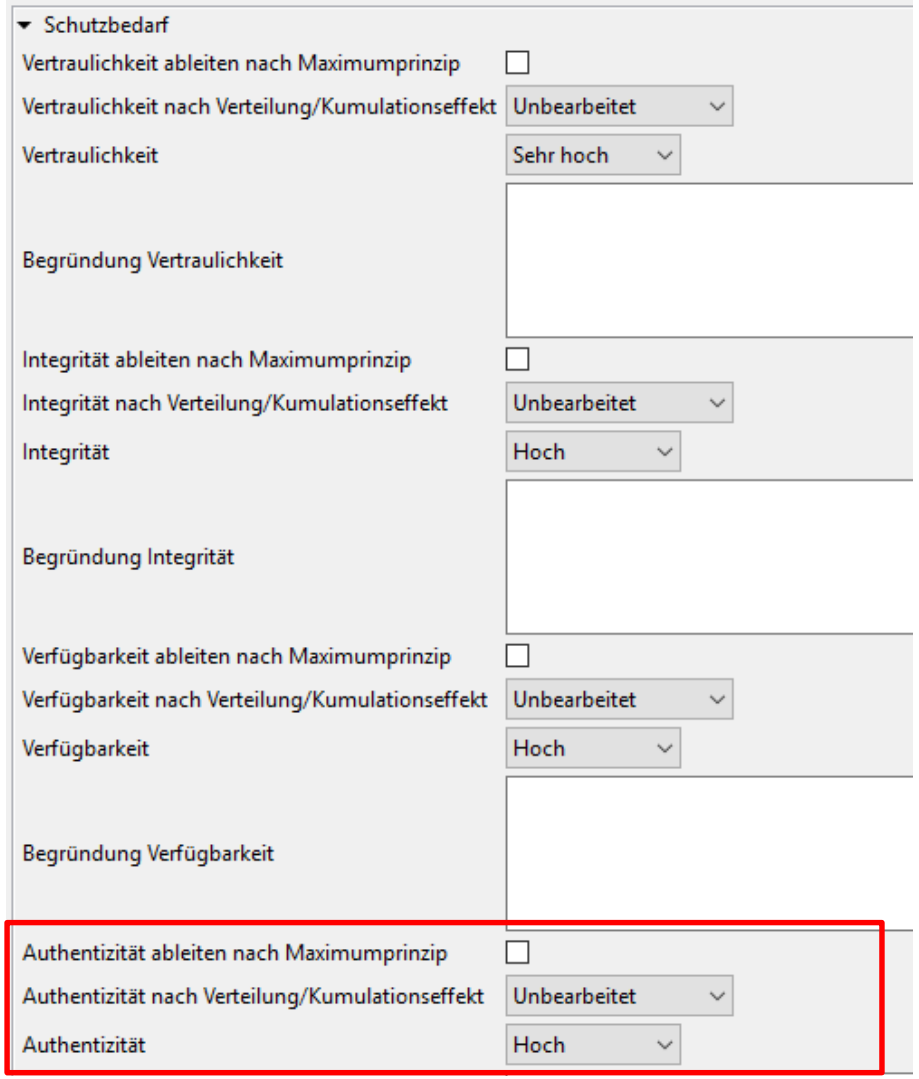
- IT-Systeme in Gruppen zusammengefasst
- Kriterien:
  - Betriebssystem
  - Virtuell / physisch
  - Netz



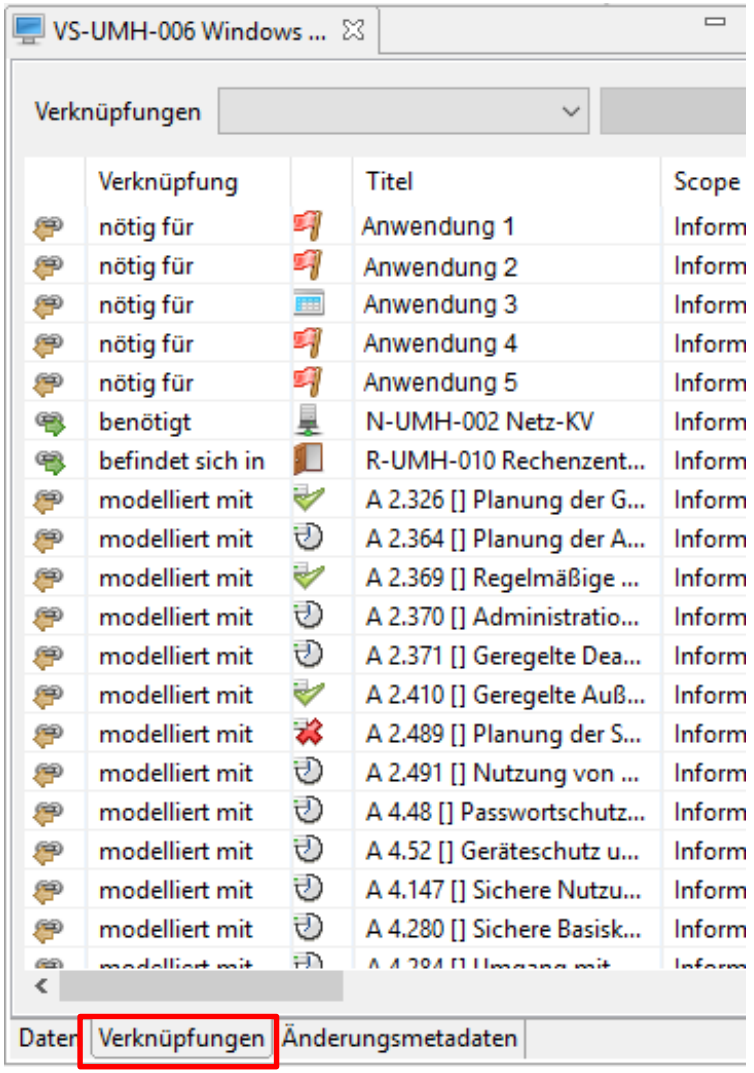


- Einfügen des zusätzlichen Schutzziels: Authentizität
- Erstellung von eigenen Bausteinen für Labor- und Medizingeräte
  - SYS.4.3 eingebettete Systeme (angepasst)
  - SYS.4.4 Medizingerät (aus Baustein IoT-Gerät)
- Markierung aller Scope (KRITIS) - relevanten Anwendungen



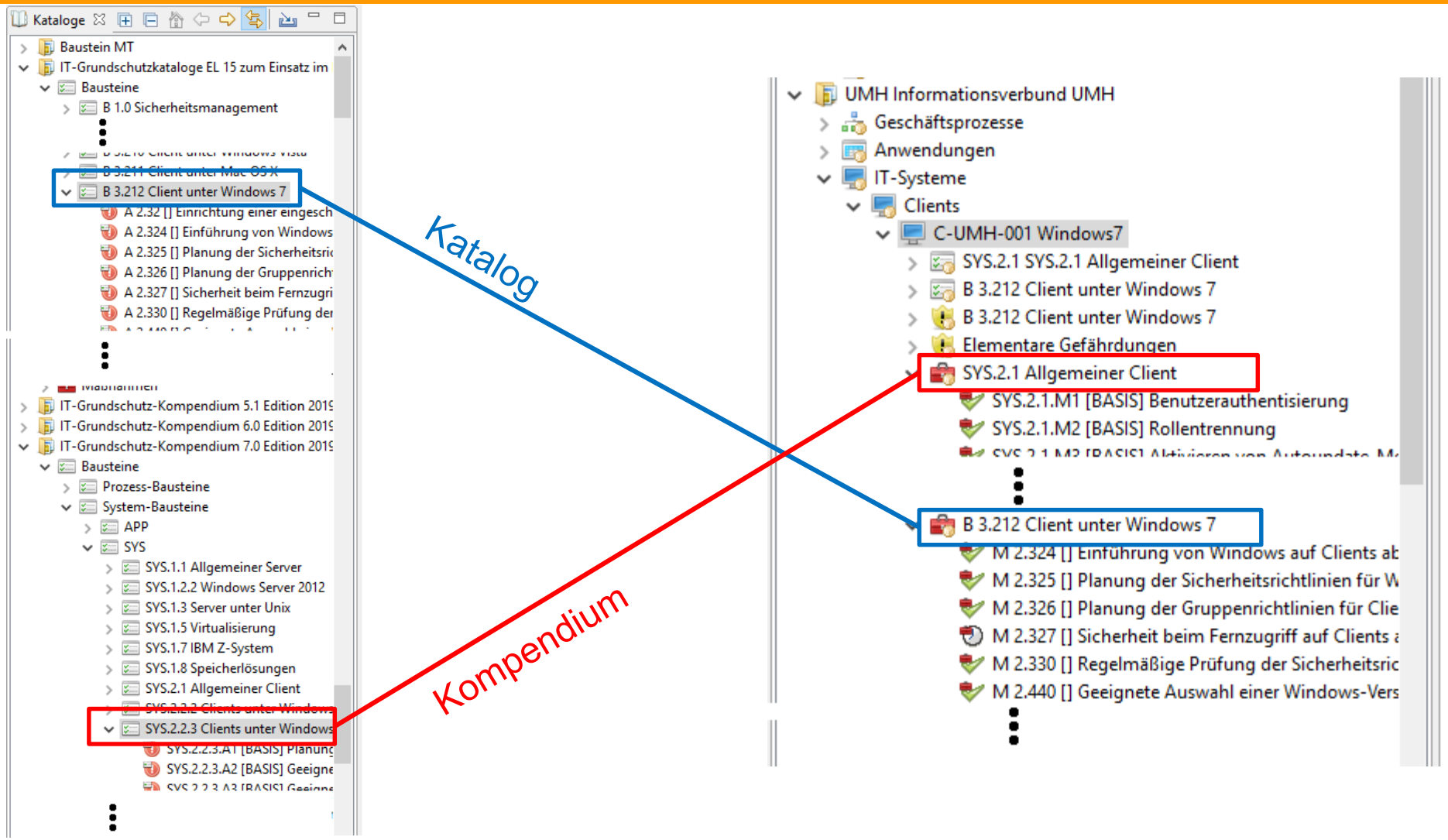


- Nötig für:
  - z.B. Anwendung
- Benötigt:
  - z.B. Kommunikationsverbindung
- Befindet sich in:
  - z.B. Raum
- Modelliert mit:
  - z.B. Anforderungen
- Beeinflusst durch:
  - z.B. Gefährdungen




BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise
IT-Sicherheitsmanagement
Initiierung Sicherheitsprozess
IT-Sicherheitsleitlinie und -konzeption:
IT-Strukturanalyse
Schutzbedarfsfeststellung
Modellierung
Basis-Sicherheitscheck
Risikoanalyse
Realisierung
Aufrechterhaltung

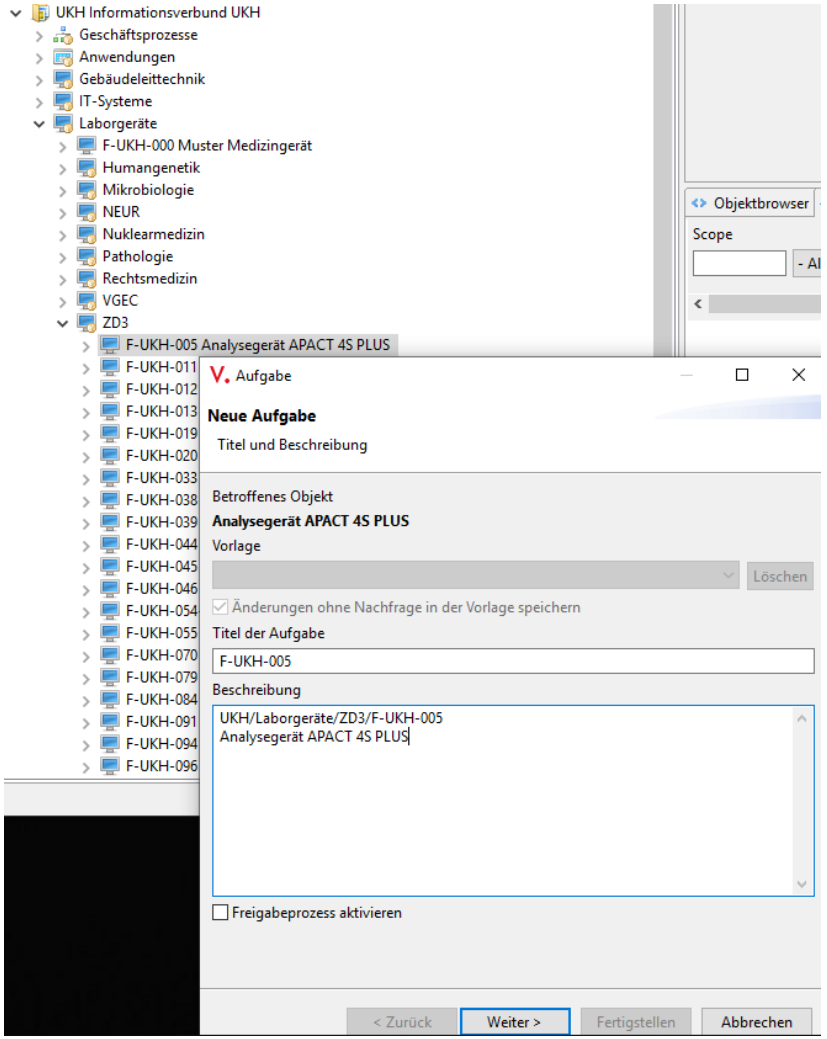
3.3 Modellierung mit dem IT-Grundschutz-Kompendium



- 70 Nutzer-Accounts im Verinice
  - IT-Beauftragte/Koordinatoren und Laborleiter
  - Administratoren
- Dokumentation **nicht** webbasiert
  - Web-Modul für Kompendium noch nicht praktikabel
- **Nachteil:**
  - Nutzer sehen nicht nur ihre IT-Systeme
  - Berechtigungen pro Informationsverbund
- **Vorteil:**
  - Nutzer sehen Dokumentation anderer IT-Systeme

3.4 Aufgaben

- Alle IT-Beauftragten sind als Nutzer in Verinice angelegt
- So können ihnen Aufgaben zugewiesen werden
- Sie werden per Mail darüber informiert

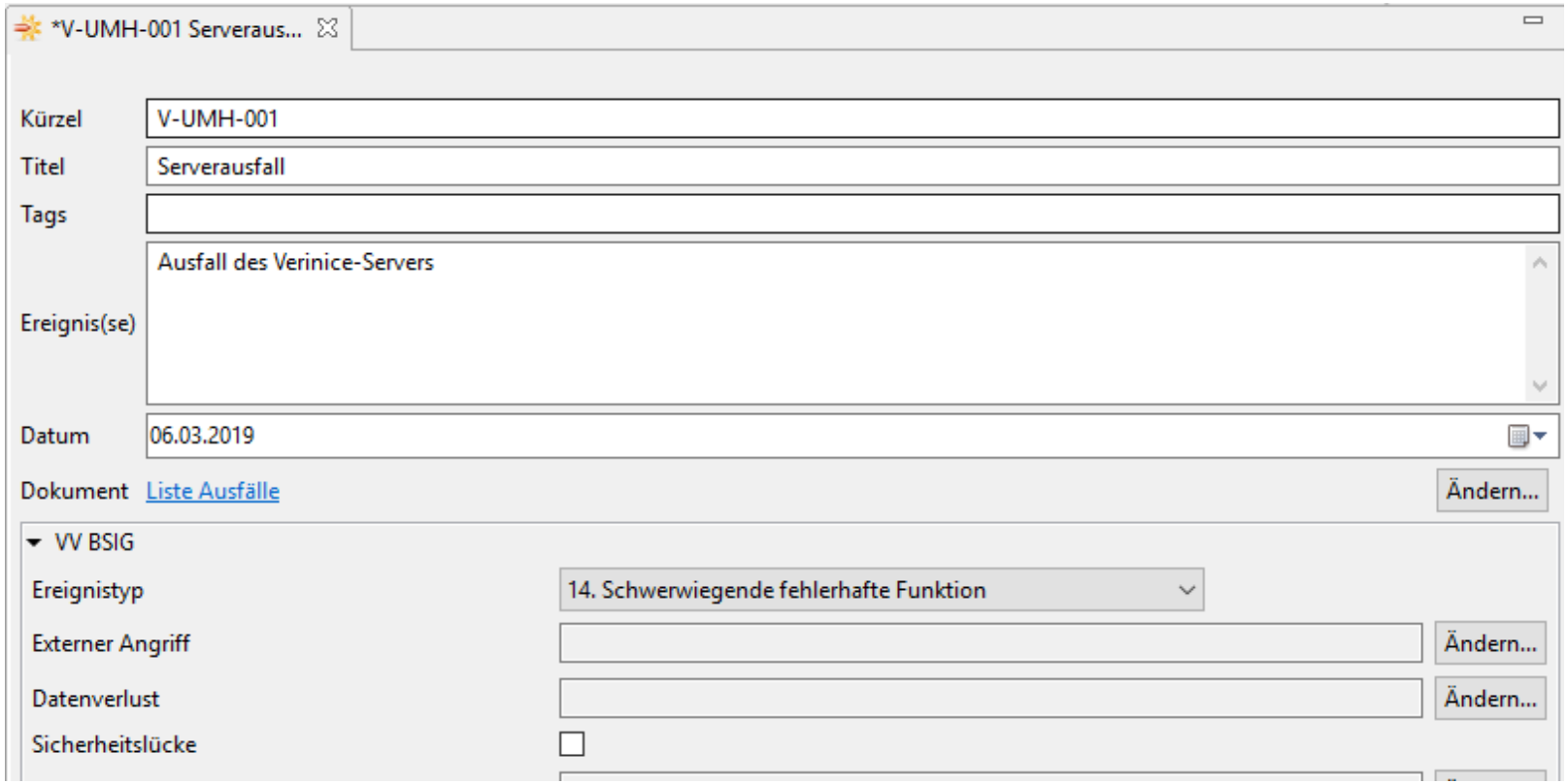


- Dokumentation durch IT-Beauftragte der Einrichtungen
  - Schwierig, da unterschiedliche IT-Kenntnisse
  - Zeitaufwendig
- Erstellung von Musterbausteinen
  - Zur Hilfestellung für die IT-Beauftragten
- Erstellung von Standard-Bausteinen für Server
  - Maßnahmen die generell für alle Server gelten, müssen nur einmal dokumentiert werden
  - Gilt für alle Server der Universitätsmedizin (Richtlinien)

- Informationsverbünde konnten klar strukturiert gezeigt werden
- Verknüpfungen zwischen den Komponenten wichtig
- Markierung der Scope-relevanten Anwendungen fehlte
- Aufstellungsort des einzelnen IT-Systems war noch nicht vorhanden
- Dokumentation und Umsetzung der Maßnahmen noch nicht abgeschlossen

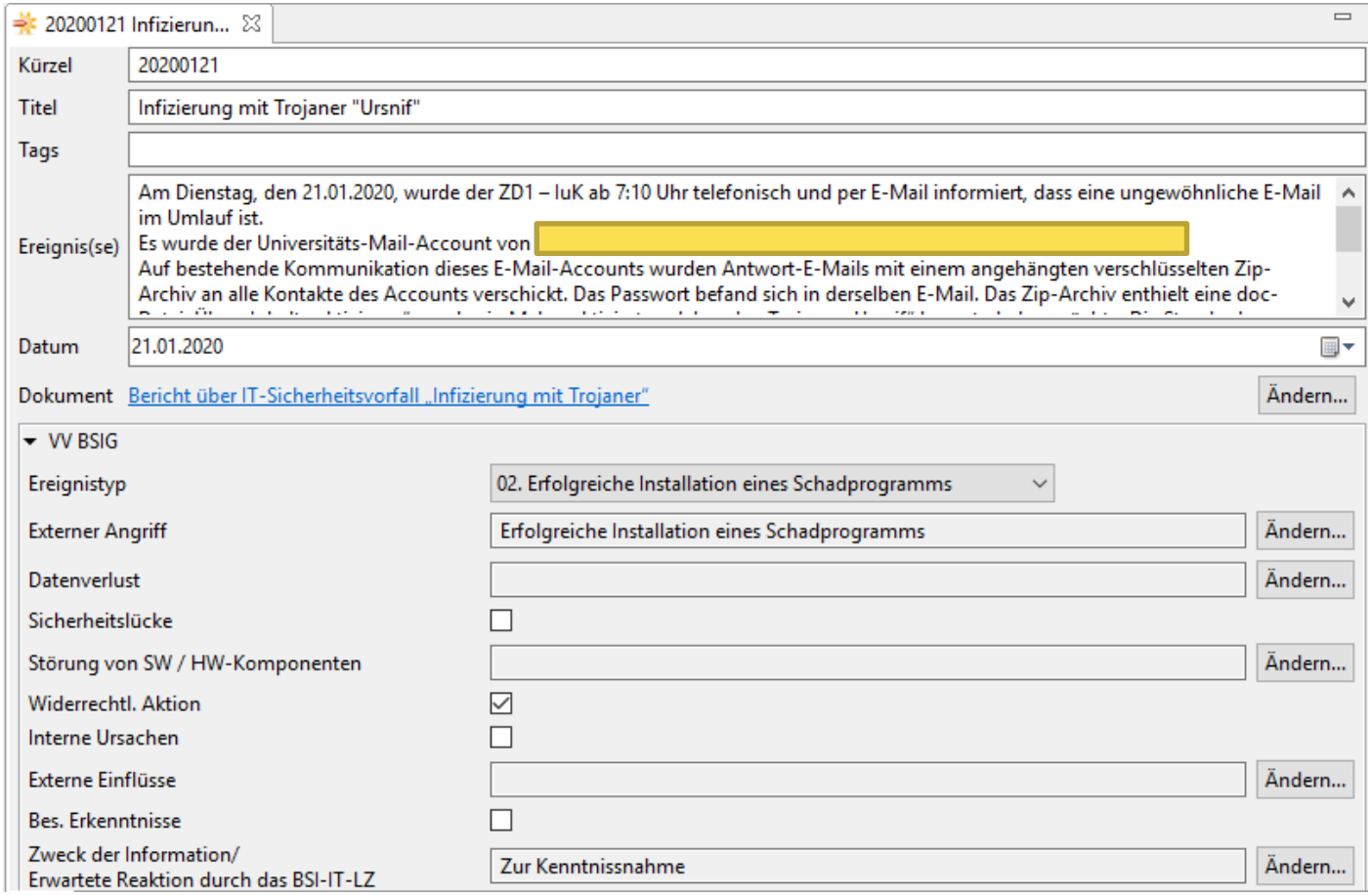
Bundesamt für Sicherheit in der Informationstechnik

1. Systemausfälle



- Keine Angabe von Uhrzeit / Örtlichkeit etc. möglich

2. Vorfälle mit Meldung an das BSI



- Erstellung von Reports
  - Reportvorlagen nicht praktikabel
  - Angepasste Reports auf unsere Fragestellungen / IT-Systeme
- Risikoanalyse
  - Bisher Excel-basiert
- Datenschutz
  - Erfassung der Verfahrensverzeichnisse

4. Wünsche an SerNet (Verinice)

- Automatische Aktualisierung der modellierten Bausteine, wenn ein neuer Katalog vom BSI veröffentlicht wird
- Anpassung des web-Moduls an IT-Grundschutz Kompendium
- Seit 1.1.2020 Aufgabengebiet der Universitätsmedizin auf Informationssicherheit erweitert

  → wie kann ich das speziell in Verinice abbilden?

de.wikipedia.org

DANKE

https://www.merseburg.de/de/hallesaale/halle-saale.html

https://www.merseburg.de/de/hallesaale/halle-saale.html

Dr. Susanne Aust

27. Februar 2020

Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg

UKH
Universitätsklinikum
Halle (Saale)