

verinice.XP

Modernisierter IT-Grundschutz

am Beispiel des Universitätsklinikums Halle (Saale)

Susanne Aust
27.02.2020

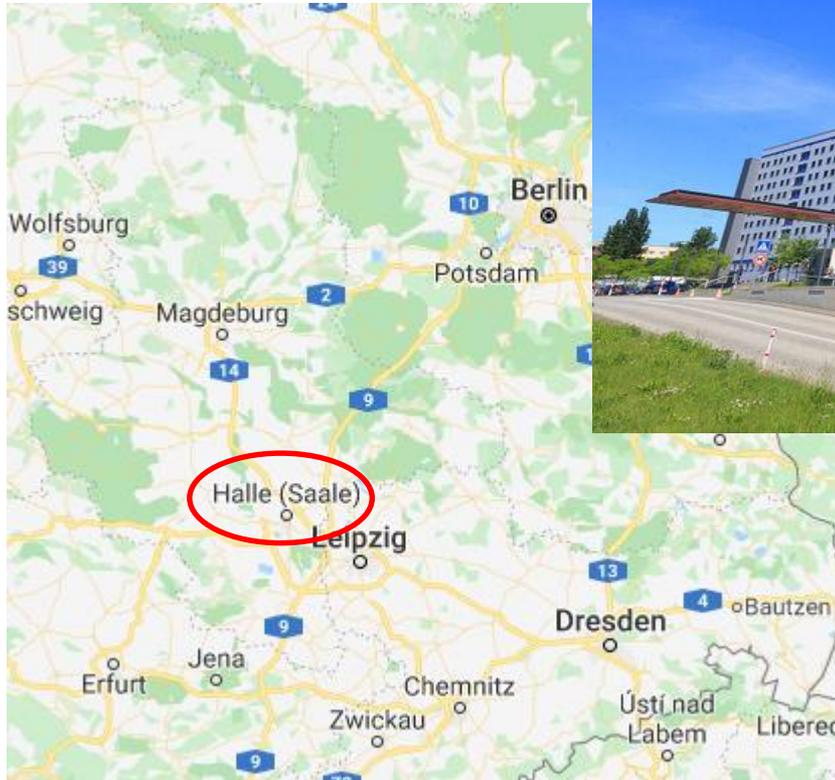


Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg

 **UKH**
Universitätsklinikum
Halle (Saale)

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

Dr. Susanne Aust
27. Februar 2020



Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg

UKH
Universitätsklinikum
Halle (Saale)

3 Standorte

Klinikum

Psychiatrie

Fakultät



Dr. Susanne Aust

27. Februar 2020



Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg



Universitätsklinikum
Halle (Saale)

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



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

Dr. Susanne Aust

27. Februar 2020



Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg



Universitätsklinikum
Halle (Saale)

Unterstützung durch die Firma Sila Consulting



Dr. Susanne Aust

27. Februar 2020

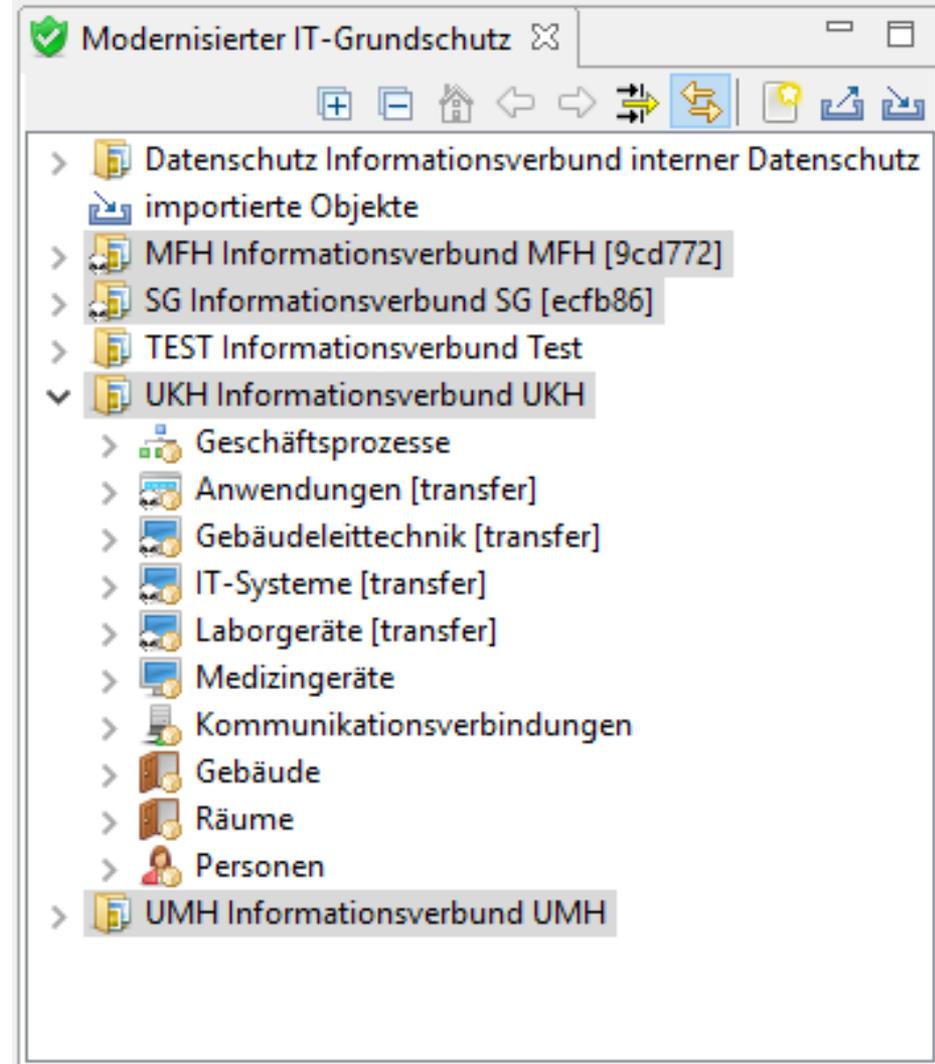


Medizinische Fakultät
der Martin-Luther-Universität
Halle-Wittenberg

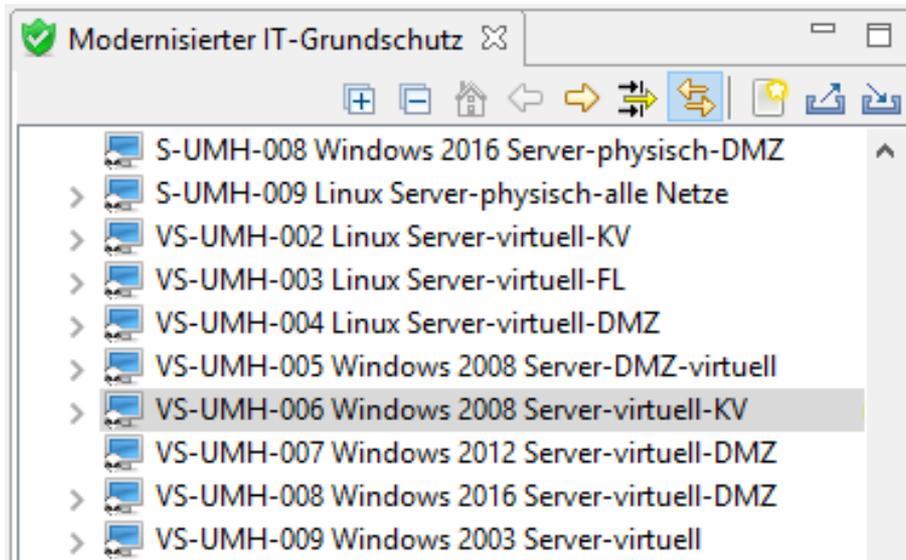


Universitätsklinikum
Halle (Saale)

- 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



VS-UMH-006 Windows ...

Kürzel: VS-UMH-006

Titel: Windows 2008 Server-virtuell-KV

Medizinprodukt-ID:

Tags:

Beschreibung: Servername 1, Servername 2, Servername 3, Servername 4, Servername 5

Plattform / Baustein: Windows Server 2008

Aufstellungsort: EGS, VM

Anzahl: 19

Status: Betrieb

Netzadressen:

Interfaces:

Benutzer: Leiter Anwendungen

Dokument:

Schutzbedarf

Vertraulichkeit ableiten nach Maximumprinzip

Daten Verknüpfungen Änderungsmetadaten

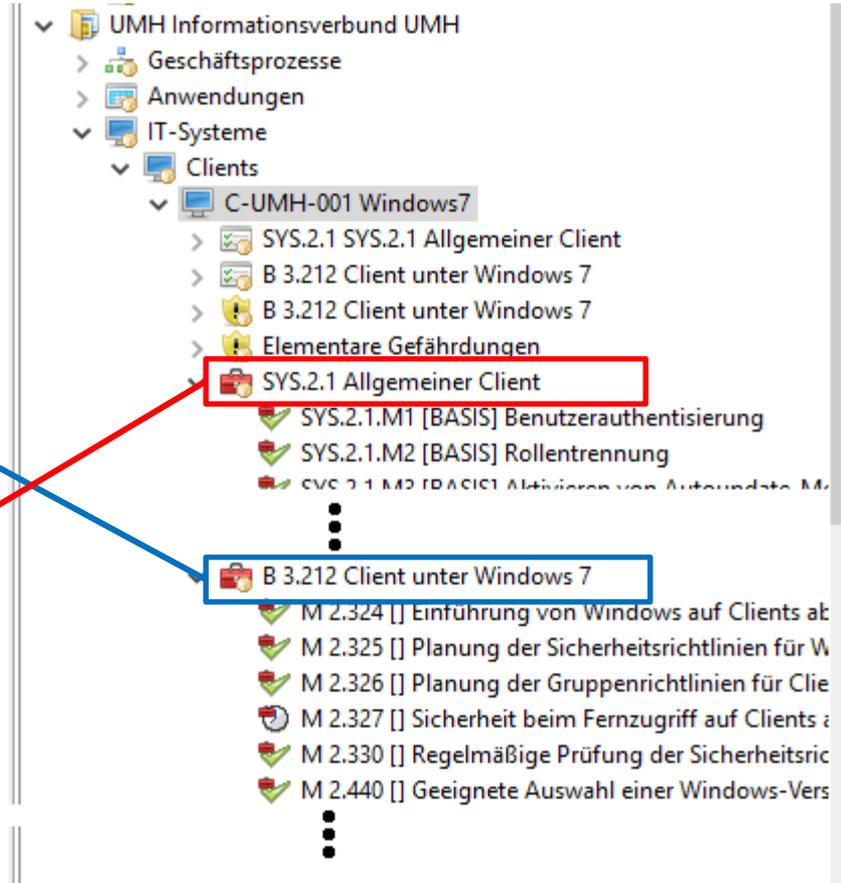
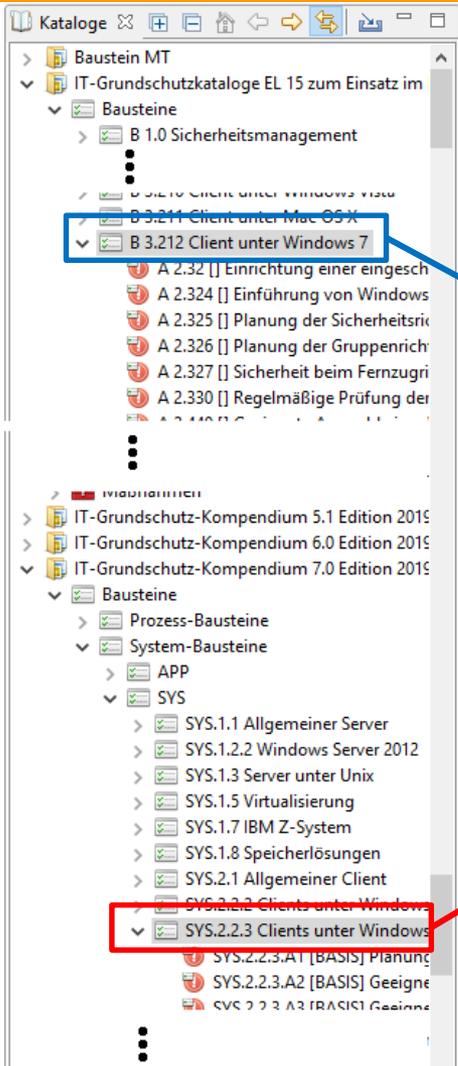
- Einfügen des zusätzlichen Schutzziels: Authentizität
- Erstellung von eigenen Bausteinen für Labor- und Medizingeräte
 - SYS.4.3 eingebettete Systeme (angepasst)
 - SYS.4.4 Medizingerät (aus Baustein IoT-Gerät)
- Markierung aller Scope (KRITIS) - relevanten Anwendungen
 - >  A-UMH-054 Office
 - >  A-UMH-055 Outlook
 - >  A-UMH-057 MobiDik
 - >  A-UMH-058 Verinice

▼ Schutzbedarf	
Vertraulichkeit ableiten nach Maximumprinzip	<input type="checkbox"/>
Vertraulichkeit nach Verteilung/Kumulationseffekt	Unbearbeitet ▼
Vertraulichkeit	Sehr hoch ▼
Begründung Vertraulichkeit	
Integrität ableiten nach Maximumprinzip	<input type="checkbox"/>
Integrität nach Verteilung/Kumulationseffekt	Unbearbeitet ▼
Integrität	Hoch ▼
Begründung Integrität	
Verfügbarkeit ableiten nach Maximumprinzip	<input type="checkbox"/>
Verfügbarkeit nach Verteilung/Kumulationseffekt	Unbearbeitet ▼
Verfügbarkeit	Hoch ▼
Begründung Verfügbarkeit	
Authentizität ableiten nach Maximumprinzip	<input type="checkbox"/>
Authentizität nach Verteilung/Kumulationseffekt	Unbearbeitet ▼
Authentizität	Hoch ▼

- 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

Verknüpfung	Titel	Scope
nötig für	Anwendung 1	Inform
nötig für	Anwendung 2	Inform
nötig für	Anwendung 3	Inform
nötig für	Anwendung 4	Inform
nötig für	Anwendung 5	Inform
benötigt	N-UMH-002 Netz-KV	Inform
befindet sich in	R-UMH-010 Rechenzent...	Inform
modelliert mit	A 2.326 [] Planung der G...	Inform
modelliert mit	A 2.364 [] Planung der A...	Inform
modelliert mit	A 2.369 [] Regelmäßige ...	Inform
modelliert mit	A 2.370 [] Administratio...	Inform
modelliert mit	A 2.371 [] Geregelte Dea...	Inform
modelliert mit	A 2.410 [] Geregelte Auß...	Inform
modelliert mit	A 2.489 [] Planung der S...	Inform
modelliert mit	A 2.491 [] Nutzung von ...	Inform
modelliert mit	A 4.48 [] Passwortschutz...	Inform
modelliert mit	A 4.52 [] Geräteschutz u...	Inform
modelliert mit	A 4.147 [] Sichere Nutzu...	Inform
modelliert mit	A 4.280 [] Sichere Basisk...	Inform
modelliert mit	A 4.281 [] Umgang mit	Inform

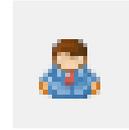




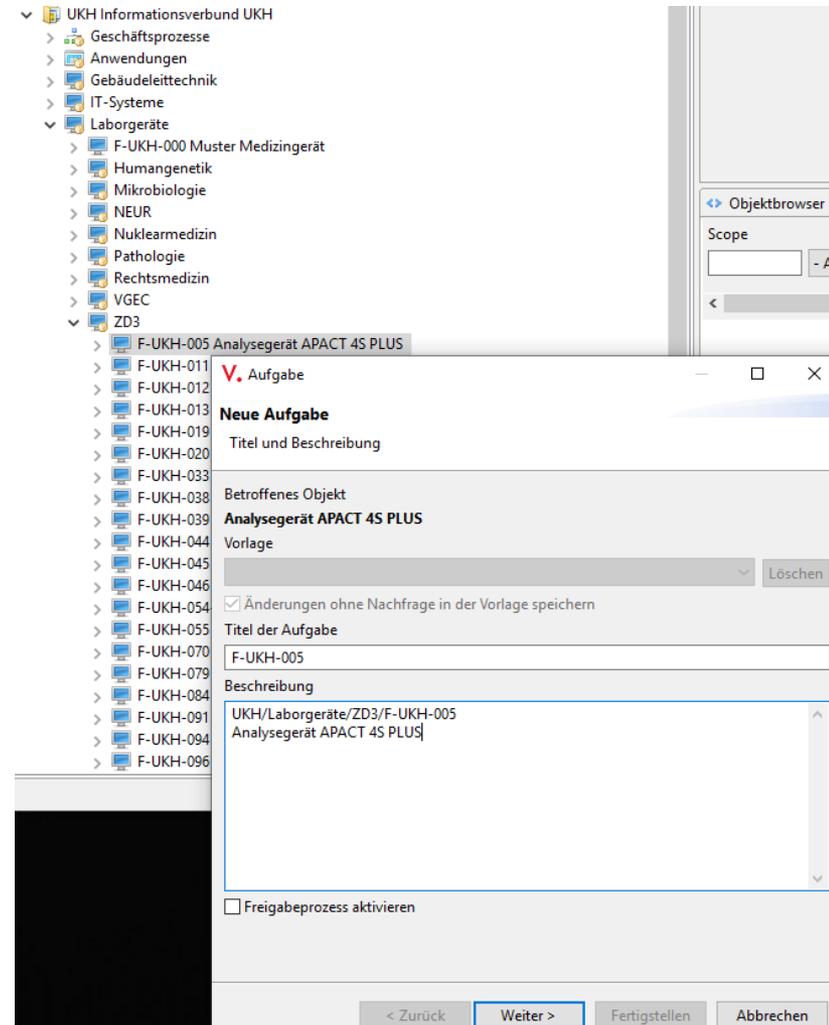
Katalog

Kompodium

- 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



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



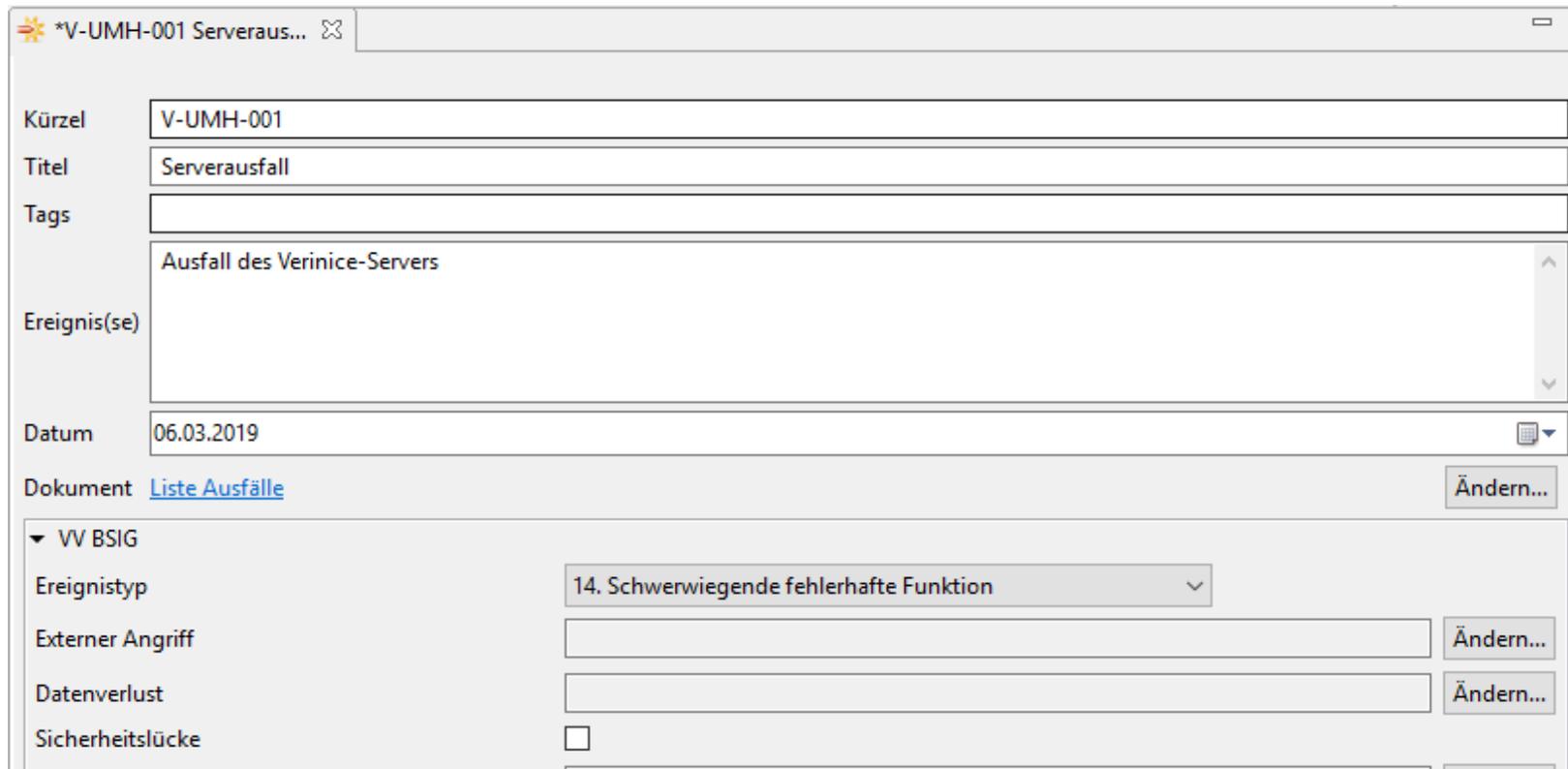
- Dokumentation durch IT-Beauftragte der Einrichtungen
 - Schwierig, da unterschiedliche IT-Kenntnisse
 - Zeitaufwendig
- Erstellung von Musterbausteinen
 - Zur Hilfestellung für die IT-Beauftragten
- Erstellung von Standard-Bausteinen für Server
 - Maßnahmen die generell für alle Server gelten, müssen 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



*V-UMH-001 Serveraus...

Kürzel: V-UMH-001

Titel: Serverausfall

Tags:

Ereignis(se): Ausfall des Verinice-Servers

Datum: 06.03.2019

Dokument: [Liste Ausfälle](#) Ändern...

▼ VV BSIG

Ereignistyp: 14. Schwerwiegende fehlerhafte Funktion

Externer Angriff: Ändern...

Datenverlust: Ändern...

Sicherheitslücke:

- Keine Angabe von Uhrzeit / Örtlichkeit etc. möglich

2. Vorfälle mit Meldung an das BSI

☀ 20200121 Infizierun... ☒	
Kürzel	20200121
Titel	Infizierung mit Trojaner "Ursnif"
Tags	
Ereignis(se)	Am Dienstag, den 21.01.2020, wurde der ZD1 – luK ab 7:10 Uhr telefonisch und per E-Mail informiert, dass eine ungewöhnliche E-Mail im Umlauf ist. Es wurde der Universitäts-Mail-Account von [REDACTED] Auf bestehende Kommunikation dieses E-Mail-Accounts wurden Antwort-E-Mails mit einem angehängten verschlüsselten Zip-Archiv an alle Kontakte des Accounts verschickt. Das Passwort befand sich in derselben E-Mail. Das Zip-Archiv enthielt eine doc-
Datum	21.01.2020
Dokument	Bericht über IT-Sicherheitsvorfall „Infizierung mit Trojaner“ Ändern...
▼ VV BSIG	
Ereignistyp	02. Erfolgreiche Installation eines Schadprogramms
Externer Angriff	Erfolgreiche Installation eines Schadprogramms Ändern...
Datenverlust	<input type="text"/> Ändern...
Sicherheitslücke	<input type="checkbox"/>
Störung von SW / HW-Komponenten	<input type="text"/> Ändern...
Widerrechtl. Aktion	<input checked="" type="checkbox"/>
Interne Ursachen	<input type="checkbox"/>
Externe Einflüsse	<input type="text"/> Ändern...
Bes. Erkenntnisse	<input type="checkbox"/>
Zweck der Information/ Erwartete Reaktion durch das BSI-IT-LZ	Zur Kenntnissnahme Ändern...

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



- 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)