Anforderungen an die Modellierung von IT-Sicherheitszonen in 3LGM²

Sönke Fischer[a], Alfred Winter[b], Björn Bergh[a], Alexander Strübing[b], Angela Merzweiler[c], Martin Bialke[d], Robert Gött[d], Knut Kaulke[e], Sebastian Stäubert[b]

[a]Institut für Medizinische Informatik und Statistik, Christian-Albrechts-Universität zu Kiel und Universitätsklinikum Schleswig-Holstein; [b]*Institute for Medical Informatics, Statistics and Epidemiology (IMISE), Leipzig University, Germany;* [c]*Institut für Medizinische Informatik, Universitätsklinikum Heidelberg;* [d]*TMF e.V.;* [e]*Institut für Community Medicine, Universitätsmedizin Greifswald K.d.ö.R*

Hintergrund

Soll der IST-Zustand einer IT-Architektur dargestellt oder ein SOLL-Zustand geplant und analysiert werden, bietet das 3-Ebenen Metamodell (3LGM²) eine Methodik zur Modellierung von Informationssystem-Architekturen (IS-A) im Gesundheitswesen. Das 3LGM²-Tool implementiert diese Methodik und ermöglicht es, Modelle der IS-A, z.B. eines Krankenhauses oder einer Forschungsinfrastruktur, zu erstellen. Im Projekt 3LGM2IHE geht es u.a. um die Abbildung von IT-Sicherheitszonen.

Das 3LGM²-Tool soll bei der Modellierung komplexer IT-Verbünde wie Datenintegrationszentren (DIZ) oder KI-Umgebungen behilflich sein, in denen IT-Sicherheit eine große Rolle spielt.

Ziele und Anforderungen

Für die Modellierung von IT-Sicherheitszonen in 3LGM²-Tool wurden Anforderungen durch Literaturrecherche und die Befragung von IT-Sicherheitsexperten erhoben und hinsichtlich der Implementierung in 3LGM² untersucht. Im 3LGM²-Tool soll folgendes möglich sein:

a) Elemente allgemein in Gruppen zusammenfassen

b) Gruppen sollen durch Attribute als IT-Sicherheitszone ausgezeichnet und näher beschrieben werden können.

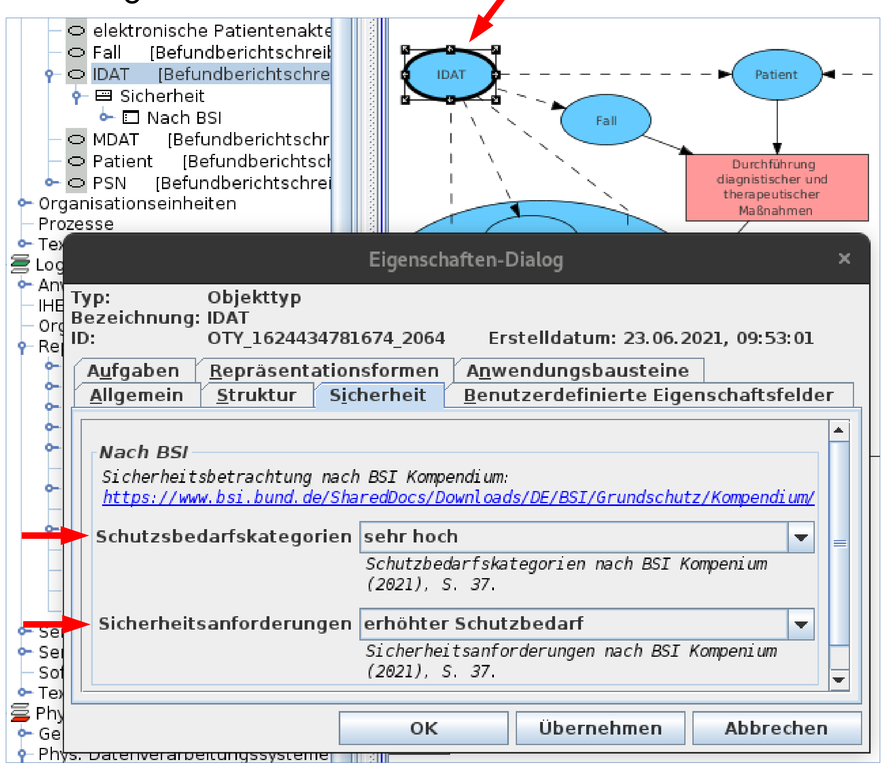
c) Attribute (=Metadaten einer IT-Sicherheitszone) sind spezifizierbar

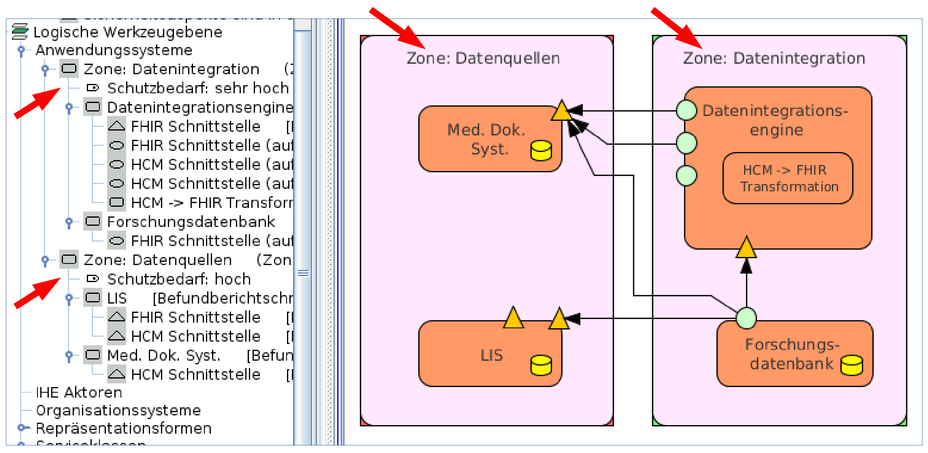
d) Für häufige Kombinationen aus Gruppen & Attributen sollen Vorlagen entwickelt werden (schnellere, einheitliche Modellierung)

Ergebnisse

1. Fachliche Ebene

Attribute, wie Schutzbedarfskategorie und Sicherheitsanforderungen lassen sich zu Informationsobjekten hinterlegen.





2. Logische Werkzeugebene

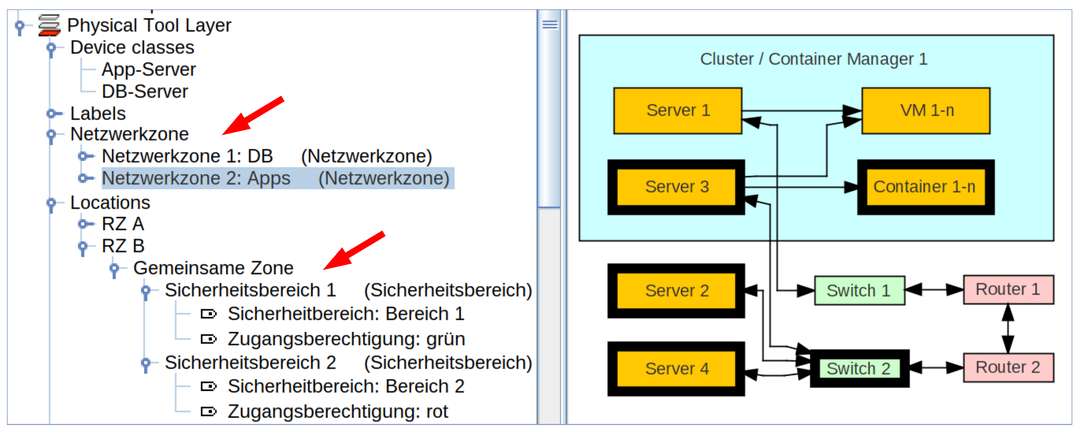
Anwendungssystem lassen sich zu IT-Sicherheitszonen gruppieren. Attribute können für diese vergeben werden, z.B. Schutzbedarf: ‚sehr hoch'.

Die Gruppen können visualisiert werden, z.B. durch Umrandung oder alternativ durch Hervorhebung (falls Anwendungssysteme visuell nicht überschneidungsfrei umrandet werden können).

3. Physische Werkzeugebene

Hierbei sind 2 Aspekte wichtig:

1. Netzwerkzonen: diese können Datenverarbeitungsbausteine (pDV) beliebig kombiniert enthalten (virtualisiert oder nicht).
2. Sicherheitsbereiche (für den Zugang zum Rechenzentrum): pDV (nicht virtuell) können genau einem Sicherheitsbereich zugeordnet werden.



Diskussion und Ausblick

Erste Untersuchungen zu den Metadaten von IT-Sicherheitszonen zeigten, dass es kein einheitliches Verständnis darüber gibt. Je nach Fokus können unter dem Begriff "IT-Sicherheitszone" u.a. räumliche, personelle oder technische Aspekte verstanden werden. Des Weiteren sind beim Aufbau, dem Betrieb und der Kontrolle von IT-Sicherheitszonen unterschiedliche Personengruppen involviert. Dazu gehören u.a. IT-Administratoren (mit unterschiedlichen Tätigkeitsfeldern und Spezialisierungen), Anwendungsbetreuer, Informationssicherheitsbeauftragte und Datenschutzbeauftragte - alle mit einer besonderen, u.U. zu den anderen verschiedenen Sicht auf das Thema. Eine Quelle für die Auswahl geeigneter Metadaten ist z.B. das Grundschutzkompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI), welches u.a. Begriffe definiert, wie Schutzbedarfsklassen ("normal", "hoch" und "sehr hoch"), die in der Implementierung Berücksichtigung finden sollen.

Dieses Poster stellt zukünftige Modellierungsmöglichkeiten im 3LGM²-Tool (Mockups) dar, welche im nächsten Release implementiert werden.

Weitere Anforderungen sollen zur iterativen Optimierung ermittelt werden, sodass sich IT-Sicherheitszonen optimal modellieren lassen. Bereits vorhandene Software-Werkzeuge, wie z.B. verinice oder CRISAM, sollen dadurch nicht ersetzt sondern vielmehr ergänzt werden.

http://www.imise.de

FKZ: BE3663/2-2, BI1930/2-2, ME5367/1-2, WI1605/9-2

http://www.3lgm2.de

Kontakt: Sebastian Stäubert, sebastian.staeubert@imise.uni-leipzig.de, IMISE Universität Leipzig, Härtelstr. 16-18, 04107 Leipzig, Germany