Entwicklung eines Prototypen zur Steigerung der Effizienz im Umgang mit den KRITIS-relevanten ISO/IEC 27K-Normen für die Anspruchsgruppe ISMS-Mitwirkende

Philipp Schütz[1], René Treibert[1], Jaroslaw Kopowski[1]

[1] Hochschule Niederrhein University of Applied Sciences, Clavis - Kompetenzzentrum für Informationssicherheit, Mönchengladbach, Deutschland
{philipp.schuetz,rene.treibert}@hs-niederrhein.de {jaroslaw.kopowski}@stud.hn.de

Abstract. Die nationale Gesetzgebung hat mit dem IT-Sicherheitsgesetz für die Betreiber von Kritischen Infrastrukturen einen legislativen Rahmen geschaffen, welcher die gesellschaftlich relevanten informationstechnischen Infrastrukturen härten soll. Die Anforderungen dieses Gesetzes allokieren bei den Betreibern i. d. R. technische und organisatorische Ressourcen. Daher ist für die Betreiber eine effiziente Implementierung der gesetzlich induzierten Anforderungen, welche sich im Wesentlichen durch die Implementierung von Anforderungen aus der Norm ISO/IEC 27001 widerspiegeln, ein Erfolgsfaktor. Der Prototyp, als ein Artefakt des Erkenntnisprozesses aus Begleitforschungen bei KRITIS-Betreibern, soll die Implementierung durch eine Suche-sensitive Zusammenstellung der KRITIS-relevanten Normen effizienzsteigernd begünstigen.

Keywords: KRITIS, ISMS, ISO27k, ISO27k-Prototyp, ISO27k-Werkzeug, IT-Sicherheitsgesetz

1 Einleitung

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (folgend IT-SiG) vom 17. Juli 2015 finden derzeit und zukünftig umfangreiche, u. a. Gesetzgeber induzierte Aktivitäten zur Steigerung der Robustheit sog. 'Kritischer Infrastrukturen' (KRITIS) statt. Um einem Ausfall oder einer Beeinträchtigung entgegenzuwirken, hat das Bundesministerium des Inneren (BMI) eine Strategie zum Schutz Kritischer Infrastrukturen entwickelt.

Aus Sicht der durch quanitative und qualitative Schwellwerte zu determinierenden KRITIS-Betreiber, wie bspw. Energieversorgern, Wasserversorgern und Krankenhäusern, lässt sich der ökonomische Aufwand zur Erfüllung der Anforderungen aus dem IT-SiG im Wesentlichen durch die Aufwände der Implementierung eines ISO/IEC 27001-konformen

Multikonferenz Wirtschaftsinformatik 2018,
March 06-09, 2018, Lüneburg, Germany

Informationssicherheitsmanagementsystems (ISMS) quantifizieren. Je nach zu betrachtendem KRITIS-Sektor bzw. der zu betrachtenden KRITIS-Betreiber-Domäne werden die Anforderungen aus der ISO/IEC 27001 um domänenspezifische Informationen aus der ISO/IEC 27000-Familie (ISO27k) ergänzt.

2 Problemstellung und Lösungsansatz

Am Beispiel eines Energieversorgungsunternehmens (EVU) im KRITIS-Kontext bedeutet dies, dass ISMS-verantwortliche Akteure zur normgerechten Erfüllung der Anforderungen aus dem IT-SiG mindestens die folgenden Standards der ISO27k berücksichtigen sollten:

- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [1]
- ISO/IEC 27002 IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management [2]
- ISO/IEC 27005 Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement [3]
- ISO/IEC TR 27019 „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [4]

Dies sind in Summe mehrere hundert Textseiten, welche jeweils miteinander pro Themenstellung und ISMS-Kategorie manuell miteinander zu verknüpfen sind.
Hier setzt die vorliegende Forschung an. Aus dem Erkenntnisgewinn von derzeit stattfindenden, anwendungsnahen Begleitforschungsprojekten bei KRITIS-Betreibern in den Sektoren ’Energie’ und ’Medizinische Versorgung’ lässt sich die Anforderung nach einer, durch Automatisierung gestützten, effizienteren Handhabung der ISO27k ableiten.

3 Konzeptionelles und erste prototypische Implementierung

Dieser Abschnitt skizziert ausgewählte Details zu den durch Begleitforschungen erhobenen Anforderungen der KRITIS-Betreiber. Des Weiteren gibt er erste Einblicke in die strukturelle Realisierung innerhalb der Problemdomäne ISMS-Implementierung, und den Modellierungsdetails, auf der Ebene der Persistenz des Prototypen. Außerdem veranschaulicht er anhand eines praxisüblichen Anwendungsszenarios den derzeitigen Stand der ersten Laufzeitversion des implementierten Prototypen. Subsumierend beansprucht das Bündel der Anforderungen eine effizientere Handhabung der ISO27k, für die Anspruchsgruppe ISMS-Mitwirkende. Dies wird aus der Perspektive des Benutzers durch eine Filter-sensitive ISO27k-Aggregation im Prototypen ermöglicht.

3.1 Prototypengestütztes Anwendungsszenario

Gemäß der Problemstellung aus Abschnitt zwei, verwendet der Benutzer in diesem praxisnahen Szenario den Prototypen um an Informationen aus den Normen zu gelangen. Der Benutzer, er sei ein Mitwirkender bei einem EVU, welcher im Zuge der ISMS-Implementierung die Anforderungen aus dem IT-SiG normenkonform umsetzen möchte. In einer Projektsitzung des EVU wird aus der ISO/IEC 27001 der Prüfbereich (engl. Control) "Änderungssteuerung" thematisiert. Anstatt der manuellen Aggregation der physisch oder digital vorliegenden, jeweils disjunkten, ISO-Normen 27001, 27002 und 27019 (ausgedruckt oder im PDF-Format) verwendet der ISMS-Mitwirkende den Prototypen. Zur Recherche innerhalb der ISO27k hat der Benutzer grundsätzlich drei Suchoptionen (siehe Abb. 1 Anwendungsfälle – ISO27K Recherche), welche jeweils den gleichen Suchraum, bestehend aus der relational-logischen Verknüpfung der ISO-Normen 27001, 27002, 27019 sowie 27799 traversieren.

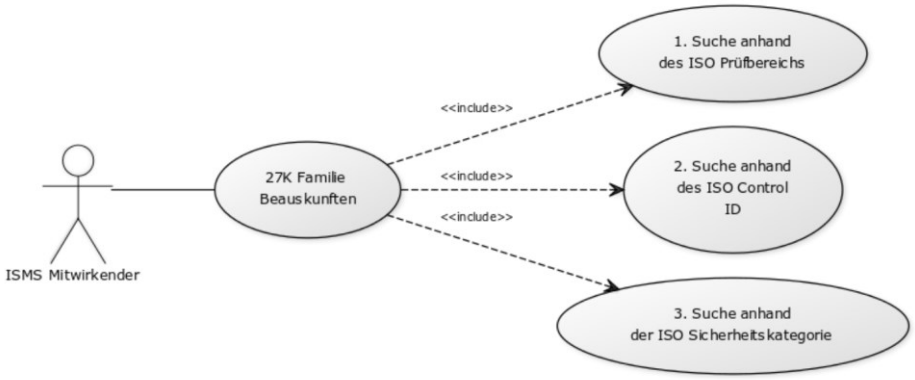

Abbildung 1. Anwendungsfälle – ISO27k Recherche

Anhand der Anwendungsfälle 1. und 2. wird das Anwendungsszenario folgend veranschaulicht.

3.2 Anwendungsfall 1: Suche anhand des ISO-Prüfbereichs

Der Benutzer wählt die ISO-Norm ‚ISO 27001' aus und hinterlegt im Suchfeld den Term „Änderungssteuerung". Die Ergebnismenge lautet: ‚Control-ID: A. 12.2.2 Änderungssteuerung'. Beim Anwählen des Hyperlinks erhält der Benutzer ein fachlich verknüpftes ISO27k-Aggregat der Inhalte, (siehe Abb. 4 Darstellung der aggregierten Ergebnismenge).

Abbildung 2. Anwendungsfall 1 – Suche anhand des ISO-Prüfbereichs

3.3 Anwendungsfall 2: Suche anhand der ISO Control-ID

Alternativ zum Anwendungsfall 1 hinterlegt der Benutzer (siehe Abb. 3 Anwendungsfall 2- Suche anhand der ISO Control-ID) im Suchfeld die Control-ID "12.1.2" zur Änderungssteuerung und wählt wieder die ISO-Norm "ISO 27001" aus. Beim Anwählen der Suche erhält der Benutzer die in der Abbildung 4 äquivalente Darstellung.

Abbildung 3. Anwendungsfall 2- Suche anhand der ISO Control-ID

3.4 Ergebnisdarstellung

Als Resultat der Suche nach der ISO-Control-ID "12.1.2" zur Änderungssteuerung bzw. der Suche nach dem Term "Änderungssteuerung" wird dem Benutzer in diesem Szenario das logisch verknüpfte Aggregat der ISO's 27001, 27002 sowie 27019 dargestellt (siehe dazu Abb. 4 Darstellung der aggregierten Ergebnismenge).

Die durch den Prototypen automatisierte Aggregation der Ergebnismenge aus den ISOs 27001, 27002 und 27019, in diesem Anwendungsfall für den KRITIS-Sektor 'Energie', führt zu erheblichen Effizienzsteigerungen in Form von Zeit, denn ISMS-Mitwirkende können sich innerhalb kürzester Zeit einen Überblick über die Inhalte und Zusammenhänge der ISO27k zusammenstellen.

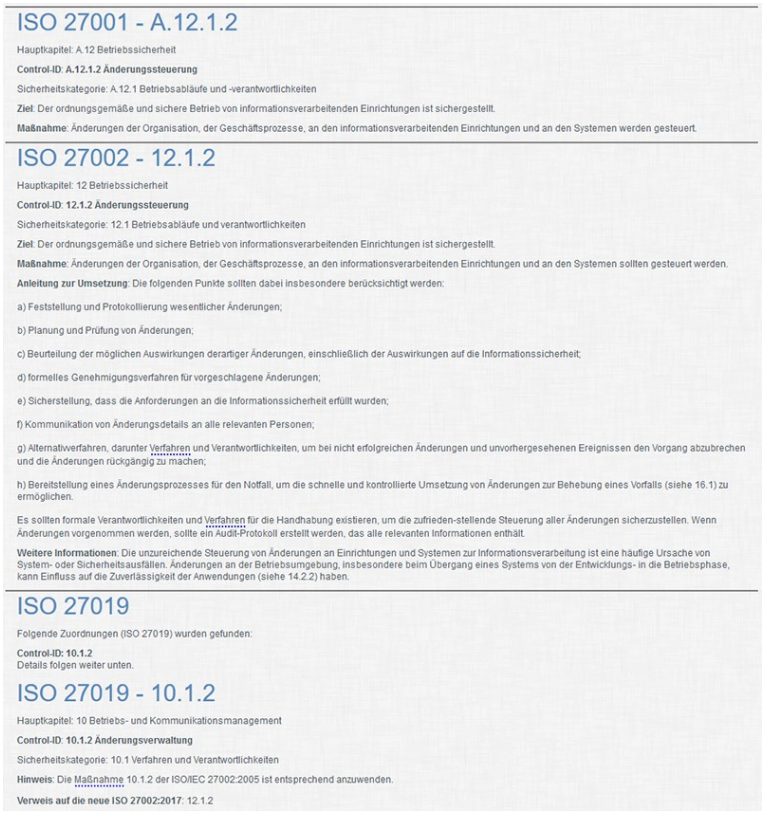

Abbildung 4. Darstellung der aggregierten Ergebnismenge,

Datenquellen [1,2,4]

3.5 Datenmodell in der Persistenz

Die folgende Tabelle 1 gibt eine Übersicht über die bereits im Prototypen implementierten ISO-Normen aus der ISO27k in der jeweiligen Version.

Tabelle 1. Im Prototypen bereits implementierte ISO-Normen der ISO27k

Norm	*Version*	*Thema*	*Internationale Norm*
ISO/IEC 27000	Juli 2011 (DE)	Überblick und Terminologie	ISO/IEC 27000:2009

ISO/IEC 27001	Juni 2017 (DE)	Anforderungen und Maßnahmen	ISO/IEC 27001:2013 einschließlich Cor1:2014 und Cor2:2015
ISO/IEC 27002	Juni 2017 (DE)	Leitfaden Maßnahmen	ISO/IEC 27002:2013 einschließlich Cor1: 2014 und Cor2: 2015
ISO/IEC 27019	März 2015 (DE)	Energieversorger	ISO/IEC TR 27019:2014
ISO/IEC 27799	Dezember 2016 (UK)	Med. Versorgung	ISO/IEC 27799:2016

Im Zuge einer Analyse wurde die ISO27k hinsichtlich ihrer Taxonomie, Verweisen, Erweiterungen sowie fachlichen Inhalten untersucht. Aus diesen Erkenntnissen wurde das relationale Datenmodell in der Abb. 5 des Prototypen iterativ entwickelt. Eine der Besonderheiten war die Implementierung der Zuordnungen der in der ISO/IEC 27019 auf die ISO/IEC 27002:2005 verwiesenen Anforderungen auf die derzeit geltende ISO/IEC 27002:2017 (DE). Im Datenmodell wird eine ISO in ihre Hauptbestandteile disaggregiert. Die ISO/IEC 27019 beispielsweise, dargestellt im Hauptentitätstypen , iso_27019‘, besteht aus den Bestandteilen (Entitätstypen): Hauptkategorie, Sicherheitskategorie, neu hinzugekommener Sicherheitskategorie und Anforderung, welche jeweils eine Erweiterung der ISO 27002 Anforderung oder eine neu hinzugefügte Anforderungen in der ISO/IEC 27019 sein kann. Die Zuordnungen (Mapping) der einzelnen Anforderungen wird im Entitätstypen “Mapping_19” im Datenmodell abgebildet. Diese Strukturwahl in der Modellierung lässt eine flexible Aggregation der Ergebnismenge zu, sowie die Integration weiterer ISO-Normen (siehe auch Abschnitt vier).

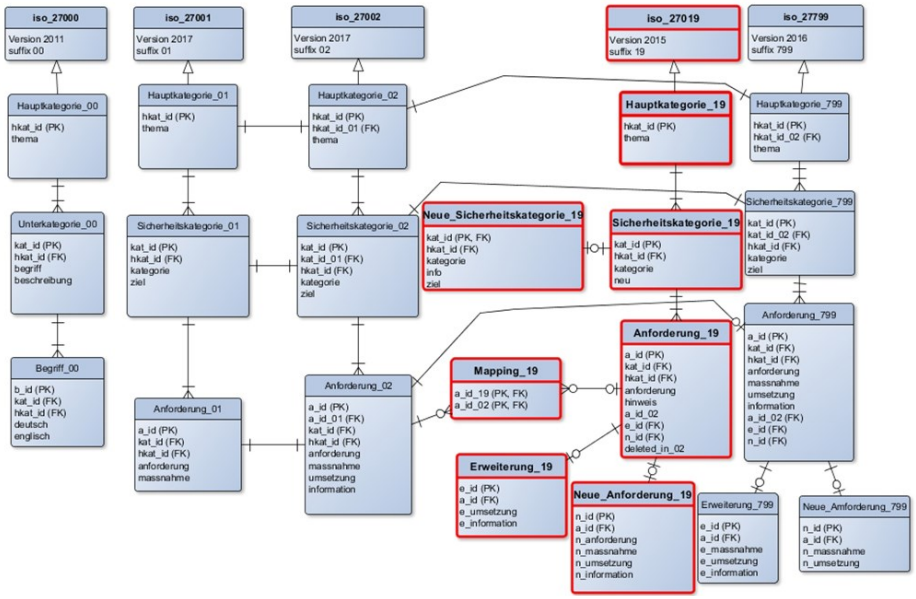

Abbildung 5. Ausschnitt des Datenmodells

3.

In Anlehnung an die normgerechten Aspekte zur Ergonomie der Mensch-System Interaktion [6] wurde am 09.11.2017 eine Erstevaluation mit einer qualifizierten Anspruchsgruppe von 13 Personen anhand des Awendungsszenarios aus den Abschnitten 3.1-3.4 durchgeführt. Die grundsätzliche Gebrauchsttauglichkeit wurde darin, relativ Ausgedrückt, mit 92,31 % bewertet. Ein Hinweis auf eine Optimierung der User Experience als Element der Zufriedenstellung war bspw., dass die Ergebnisdarstellung (siehe Abb. 4) auch hinweisgebender zwischen normativen und nicht-normativen Normen-Bestandteilen unterscheiden sollte. Neben der Gebrauchstauglichkeit wurden weitere Rückmeldungen innerhalb einer offenen Befragung in eine Residualkategorie aufgenommen. Als besonders dienliche, noch zu implementierende Funktionalität wurde eine globale Suche auf die ISO27k, unabhängig und additiv zu den Recherchemöglichkeiten geäußert (als Erweiterung der Anwendungsfälle aus Abb. 1).

4 Konklusion und Ausblick

Der ‚Research-in-Progress' Prototyp, als ein Artefakt der gestaltungsorientierten Wirtschaftsinformatik, gliedert sich in die derzeit zahlreichen Forschungsarbeiten im KRITIS-Komplex ein. Der momentane Fokus liegt auf der Anspruchsgruppe ISMS-Mitwirkende in den KRITIS-Sektoren ‚Energie' und ‚Medizinische Versorgung'. Eine Erweiterung der Funktionalitäten, bspw. zur Verwendung in allen KRITIS-Sektoren steht in Aussicht. Auch die Vergrößerung der Anspruchsgruppen, bspw. für ISMS-

Auditoren ist geplant. Bezogen auf die Phasen im Erkenntnisprozess, finden derzeit weitere Maßnahmen statt, um den Prototypen vertiefender zu evaluieren. Im 2. Quartal 2018 sollen die Funktionalitäten aus diesem Prototypen in einem weiteren, funktional umfangreicheren Prototypen, resultierend aus den Begleitforschungen, portiert werden. Dieser adressiert insbesondere EVU im KRITIS-Komplex und soll die Effizienz der ISMS-Implementierung und des ISMS-Betriebs begünstigen.

Literatur

1. ISO/IEC 27001 (2017) IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
2. ISO/IEC 27002 (2017) IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement
3. ISO/IEC 27005 (2011) IT-Sicherheitsverfahren – Informationssicherheits-Risikomanagement
4. ISO/IEC TR 27019 (2015) Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014)
5. ISO/IEC 27799 (2016) Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2016)
6. DIN EN ISO 9241-11 (2016) Ergonomie der Mensch-System-Interaktion – Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte