Sichere Informationsinfrastrukturen für kleine und mittlere Energieversorger

Julian Dax[1], Daniel Hamburg[2], Michael Kreusch[3], Benedikt Ley[1], Sebastian Pape[4], Volkmar Pipek[1], Kai Rannenberg[4], Christopher Schmitz[4] und Frank Terhaag[5]

[1] Universität Siegen, Institut für Wirtschaftsinformatik, {vorname.nachname}@uni-siegen.de
[2] TÜV Rheinland i-sec GmbH, Köln, daniel.hamburg@i-sec.tuv.com
[3] Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung, Köln, kreusch@asew.de
[4] Goethe-Universität Frankfurt am Main, M-Chair, {vorname.nachname}@m-chair.de
[5] regio iT gesellschaft für informationstechnologie mbh, Aachen, frank.terhaag@regioit.de

Abstract

Eine sicher funktionierende Energieinfrastruktur ist für fast alle Lebensbereiche unserer heutigen Gesellschaft grundlegend. Damit die Energieversorgung im Rahmen der Energiewende auch nachhaltig sichergestellt werden kann, wird auch im Energiesektor immer mehr Informations- und Kommunikationstechnik (IKT) eingesetzt. Gleichzeitig erhöht sich dadurch jedoch auch das Risiko für IT-basierte Angriffe auf die Kritische Infrastruktur. Die effektive und effiziente Absicherung der eigenen Infrastruktur vor solchen Angriffen stellt insbesondere kleine und mittelgroße Energienetzbetreiber mit begrenzten Ressourcen vor eine besondere Herausforderung. Im Forschungsprojekt SIDATE[1] setzen wir an dieser Stelle an und erarbeiten geeignete Konzepte und Werkzeuge, die kleine und mittelgroße Energieversorger bei der Verbesserung ihrer IT-Sicherheit angemessen unterstützen sollen. Der Forschungsschwerpunkt liegt dabei auf den drei Kernthemen Bewertung von IT-Sicherheit, Wissensaustausch und Zertifizierung. Wir verfolgen im Projekt eine praxisnahe Forschungsmethodik die einen intensive Einbeziehung der Energieversorger in den gesamten Forschungsprozess vorsieht.

1 Motivation

Kritische Infrastrukturen spielen eine wichtige Rolle für das Funktionieren heutiger Informationsgesellschaften. Der Schutz dieser Infrastrukturen liegt dementsprechend im Interesse der Allgemeinheit. Faktoren wie die zunehmende Komplexität der Infrastrukturen, die wachsende Abhängigkeit zwischen unterschiedlichen Infrastrukturen und der vermehrte Einsatz von

[1] http://www.sidate.org/

(mobiler) Informations- und Kommunikationstechnik (IKT) stellen hierbei eine besondere Herausforderung bei der Erreichung dieses Zieles dar. Weiterhin wird gerade im Energiesektor eine starke Änderung der Geschäftsmodelle erwartet (PwC 2014). Diese erfordert in Verbindung mit dem Einsatz von IKT nicht nur die weiter zunehmende Dezentralisierung kritischer Infrastrukturen sondern auch die Automatisierung von Abläufen zur Steigerung der Effektivität und Effizienz. Dies führt gleichzeitig aber auch zu neuen Risiken und Gefahren.

Die Betreiber im Energiesektor stehen nun vor der Problemstellung, sowohl den Schutz als auch die Wirtschaftlichkeit ihrer Infrastrukturen sicherzustellen. Dieses Spannungsfeld stellt besonders kleine und mittelgroße Energieversorger (z.B. Stadtwerke) vor neue Schwierigkeiten, die ohne fremde Unterstützung kaum zu lösen sind. Für diese Unternehmen ist es in der Regel wirtschaftlich nicht darstellbar, spezialisiertes Personal zum Schutz ihrer IKT-Infrastruktur zu beschäftigen. Auch die Anwendung und Adaption bereits existierender Kriterienkataloge zur IT-Sicherheit bspw. auf Grundlage der ISO/IEC 27001 und ISO/IEC 27002*,* sind insbesondere ohne spezifische Kenntnisse im Bereich IT-Sicherheit kaum durchführbar. Für die konkrete Umsetzung sicherheitstechnischer Maßnahmen wäre der Einsatz von Dienstleistern eine gangbare Alternative zum Aufbau eigener Ressourcen. Es ist jedoch im Interesse der Energieversorger, den grundlegenden Schutzbedarf und das Sicherheitsniveau ihrer IKT-Infrastruktur eigenständig bzw. im organisationsübergreifenden Wissens- und Erfahrungsaustausch mit anderen Energieversorgern zu ermitteln und gegebenenfalls zu erhöhen.

Das Projekt setzt sich zum Ziel, kleinen bis mittleren Betreibern von kritischen Infrastrukturen Plattformen, Werkzeuge und Modelle zur Verfügung zu stellen, die dabei helfen, selbstständig Schwachstellen zu identifizieren, geeignete Lösungsansätze zu entwickeln und effizienten Gebrauch von organisationsübergreifend vorhandenem Wissen zu machen. Dabei geht es nicht nur um Fragen technischer, sondern auch organisatorischer und prozessualer Sicherungskonzepte. Betrachtet werden dabei sowohl Sicherheitsaspekte (Ausfallrisiko, Angriffsrisiko, Schadensabwendung und -begrenzung) als auch Kooperations- und Usability-Aspekte (z.B. Aufwand, Beeinträchtigungspotenzial und Akzeptanz von Sicherheitsmaßnahmen). Personal mit allgemeinen IKT-Kenntnissen soll in die Lage versetzt werden, den Überblick über Gefährdungen zu behalten und gegebenenfalls durch das Hinzuziehen externer Experten nachhaltige Lösungen zu erarbeiten, die auch im Alltag der Organisation gelebt werden können.

2 Forschungs- und Anwendungsfeld

Der deutsche Energiemarkt zeichnet sich durch eine große Vielfalt aus. Mit der Liberalisierung des Strommarkts Ende der 90er Jahre hat sich die Zahl der Wettbewerber in diesem Bereich stark erhöht. Im April 2015 waren in Deutschland fast 1.200 Stromlieferanten und über 900 Stromnetzbetreiber tätig (BDEW 2014). Insbesondere das Verteilnetz wird dabei größtenteils von meist kleinen bis mittelgroßen kommunalen Energieversorgern (Stadtwerken) betrieben.

Durch den vermehrten Einsatz von IKT, insbesondere auch im Rahmen der Energiewende (z.B. durch eine intelligente und dezentralisierte Energienetzführung), sind die Versorgungsnetze in ihrer IKT-Vernetzung immer weniger autark und es eröffnen sich neue Möglichkeiten IKT-basierter Angriffe auf die kritische Versorgungsinfrastruktur (BNetzA 2011). Ein medienwirksamer Selbsttest der Stadtwerke Ettlingen hat deutlich gemacht, dass die notwendige Absicherung dieser Infrastruktur insbesondere bei kleinen Energieversorgern aufgrund mangelnder Ressourcen und somit fehlender Expertise unzureichend sein kann (Grefe 2014).

Mit der Verabschiedung des IT-Sicherheitsgesetzes sowie der Veröffentlichung des IT-Sicherheitskatalogs für Energieversorger der Bundesnetzagentur im Sommer 2015 wurde ein gesetzlicher Rahmen geschaffen, der die Energieversorger zur Umsetzung und Einhaltung vorgegebener Mindeststandards verpflichtet. Auch kleine Energieversorger, die über wenig Ressourcen verfügen, müssen die Vorgaben des IT-Sicherheitskataloges uneingeschränkt umsetzen müssen.

Im Forschungsprojekt wollen wir an dieser Stelle ansetzen und geeignete Konzepte entwickeln, die kleine und mittelgroße Energieversorger bei Erfüllung der gesetzlichen Vorgaben und somit bei der Verbesserung ihrer IT-Sicherheit unterstützen. Um dieses Ziel sinnvoll erreichen zu können, arbeiten wir im Projekt mit mehreren kleinen und mittelgroßen Stadtwerken zusammen, die in ihrer Organisation und Infrastruktur unterschiedlich aufgestellt sind (vgl. Tabelle 1).

	Stadtwerk A	**Stadtwerk B**	**Stadtwerk C**	**Stadtwerk D**	**Stadtwerk E**
Mitarbeiter	1.500	655	680	245	207
stromnetzrelevante Daten:					
Gesamtlänge Freileitungen (km)	541	342	260	200	59
Gesamtlänge Kabel (km)	14.640	6.250	2.192	2.884	799
Netzebenen	Höchst-, Hoch-, Mittel-, Niederspannung	Hoch-, Mittel-, Niederspannung	Hoch-, Mittel-, Niederspannung	Hoch-, Mittel-, Niederspannung	Mittel-, Niederspannung
Versorgte Einwohner (Niederspannung)	428.794	278.373	252.221	208.408	76.628

Tabelle 1: Übersicht assoziierter Energieversorger

Die Zusammenarbeit mit und Gegenüberstellung von verschiedenen Energieversorgern im Forschungsvorhaben ermöglicht es uns, Generalisierungen auf Basis einer einzelnen Organisation zu vermeiden. Für jedes beteiligte Unternehmen werden daher basierend auf den existierenden technischen und organisatorischen Begebenheiten individuelle Praktiken und Prozesse zur Umsetzung und Verbesserung von IT-Sicherheit sowie damit einhergehende Probleme untersucht.

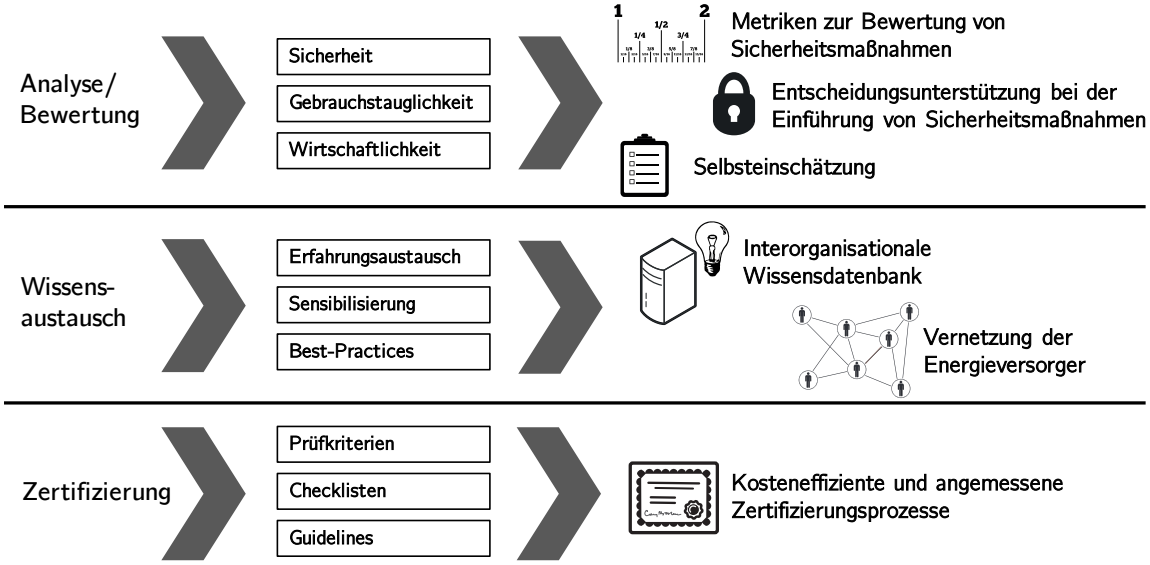

Abbildung 1: Übersicht des geplanten Forschungsvorhabens

3 Forschungsfokus und -fragen

Im Rahmen des Projekts sollen verschiedene Forschungsbeiträge entstehen. Diese konzentrieren sich im Wesentlichen auf die drei übergeordneten Kernthemen Bewertung von IT-Sicherheit, Wissensaustausch und Zertifizierung, welche in Abbildung 1 skizziert werden (vgl. Abb. 1).

Als Ausgangsbasis weiterer Forschungsschritte werden zunächst IT-sicherheitsrelevante Prozesse sowie Sicherheitsrisiken kleiner und mittlerer Energieversorger identifiziert. Darauf aufbauend werden Angriffsszenarien erarbeitet und ein Maßnahmenkatalog zur Absicherung der IKT-Infrastruktur abgeleitet.

Als zentraler Aspekt der Bewertung von IT-Sicherheit ist der Entwurf leichtgewichtiger Metriken und zugehöriger Erhebungsprozesse hervorzuheben, anhand derer das IT-Sicherheitsniveau gemessen und konkrete Sicherheitsmaßnahmen hinsichtlich ihrer Sicherheit, Gebrauchstauglichkeit und Wirtschaftlichkeit beschrieben werden können. Leichtgewichtigkeit meint, dass die Metriken auch ohne besonderen personellen oder finanziellen Ressourcenaufwand direkt durch kleine und mittlere Energieversorger anwendbar sind. Hierdurch sollen die Sicherheit, Gebrauchstauglichkeit und Wirtschaftlichkeit auch für Nicht-Experten einfach und effizient messbar werden. Dies ermöglicht eine regelmäßige Selbsteinschätzung des eigenen IKT-Sicherheitsniveaus sowie möglicher Sicherheitsmaßnahmen. Der Entwurf der Metriken, wie auch der sonstigen im Projekt entwickelten Werkzeuge, erfolgt dabei von Beginn an unter Gesichtspunkten der Nachhaltigkeit. So sollen alle entwickelten Technologien leicht an neue Technologien (z.B. Smart Meter) angepasst werden können und so nicht nur vorhandene, sondern auch sich durch Veränderungen ergebende, Systeme betrachtet werden.

1. Die quantitative Beschreibung von IT-Sicherheit stellt eine der primären Forschungsaufgaben dar. Es sollen aussagekräftige Metriken entworfen werden, um das IT-Sicherheitsniveau und konkrete Sicherheitsmaßnahmen adäquat bewerten zu können. Dies umfasst sowohl die rein technische Ebene zur Bewertung von IT-Infrastrukturen als auch die organisationale Prozessebene, um eine gesamtheitliche Perspektive auf die IT-Sicherheit einzunehmen.

   Generell lässt sich IT-Sicherheit nur schwer messen (Pfleeger 2010). Die besondere Herausforderung im Rahmen dieses Projekts besteht zusätzlich darin, Metriken zu entwickeln, die einerseits über genügend Aussagekraft besitzen, andererseits aber auch leichtgewichtig sind. Es gilt also, einen Trade-off zwischen Einfachheit der Anwendung und Genauigkeit der Ergebnisse zu finden.

2. Bedienbarkeit, Verständlichkeit und Akzeptanz von Sicherheitsmaßnahmen haben einen wesentlichen Einfluss auf das sicherheitsrelevante Nutzerverhalten. So werden Sicherheitsmechanismen, die nicht verstanden oder als störend empfunden werden, häufig durch unbewusste Fehlbedienung oder bewusstes Aushebeln wirkungslos (Whitten und Tygar 1999, Herzog 2007). Dennoch sind existierende Entwicklungsprozesse und Vorgehensmodelle des Security-Engineerings von denen des Usability-Engineerings noch immer weitgehend entkoppelt (Fischer-Hübner et al. 2011). IT-Sicherheitsverantwortliche in Unternehmen entscheiden zudem über Sicherheitsrichtlinien und -mechanismen, ohne sich der damit einhergehenden Auswirkungen auf die Arbeitspraxis der Mitarbeiter bewusst zu sein (Parkin et al. 2013).

Eine wesentliche Forschungsaufgabe im Projekt wird daher sein, solche Auswirkungen sichtbar und messbar zu machen, sodass diese bei der Auswahl geeigneter Sicherheitsmaßnahmen berücksichtigt werden können.

3. Insbesondere für kleine und mittlere Energieversorger nimmt die Wirtschaftlichkeit von Sicherheitsmaßnahmen aufgrund ihrer geringeren finanziellen Ressourcenausstattung einen hohen Stellenwert ein. Das Anspruchsvolle an der ökonomischen Bewertung von Sicherheitsmaßnahmen ist, dass durch IT-Sicherheit im Allgemeinen keine Umsätze generiert werden, sondern nur Schaden reduziert wird, der sich nicht exakt quantifizieren lässt.

   Im Projekt soll die Wirtschaftlichkeit anhand der für die Durchführung von Sicherheitsmaßnahmen anfallenden Kosten sowie deren Wirksamkeit ermittelt werden. Hierfür werden individuelle Kosten- und Wirksamkeitsfaktoren für die identifizierten Sicherheitsmaßnahmen abgeschätzt und daraus Effizienzfaktoren abgeleitet.

Darüber hinaus wird ein Konzept zur Visualisierung von Infrastrukturelementen erarbeitet, welches ihre Zusammenhänge mit Organisationseinheiten und Geschäftsprozessen darstellt und ergänzende Informationen zu IT-Sicherheitsniveau, Usability und Kosten enthält. Letztendlich sollen Entscheider hierdurch virtuell Sicherheitsmaßnahmen einführen können und die verschiedenen Auswirkungen grafisch angezeigt bekommen.

Neben der Bewertung von Sicherheitsmaßnahmen kommt dem Wissensaustausch eine essentielle Rolle zu. So soll eine organisationsübergreifende Wissensdatenbank und Austauschplattform zum Erfahrungsaustausch mit anderen Energieversorgern entstehen. Dies ist insbesondere deshalb sinnvoll, da Infrastrukturen und Risikostrukturen von Betreibern kritischer Infrastrukturen oft vergleichbar sind und Lösungsansätze somit sinnvoll wiederverwendet werden können.

In Hinblick auf die Etablierung einer solchen Plattform ist zunächst die Nutzungsbereitschaft der Energieversorger genauer zu betrachten, die sich im Sinne einer Kosten-Nutzen-Abwägung aus Nutzungsmotivation einerseits und Nutzungsaufwand und -risiken andererseits ableitet.

So stellt sich etwa die Frage, welcher Nutzungsaufwand in Bezug auf Datenerhebung und -erfassung vertretbar ist und welche Informationen über die IT-Infrastruktur, dessen Sicherheitsniveau und eingeführte Maßnahmen und Auswirkungen in der Wissensdatenbank abgelegt werden sollen. Dies umfasst auch die Entwicklung adäquater Formate und Datenstrukturen für die Speicherung relevanter Informationen sowie der Identifizierung möglicher Assoziationen zwischen verschiedenen Informationstypen.

Da die Energieversorger über die Plattform höchst sensible Informationen austauschen, sind adäquate Datenschutz- und Zugriffskontrollkonzepte zu entwickeln. Diese sollen sicherstellen, dass die Energieversorger die Kontrolle darüber haben, welche Informationen in welchem Detailgrad abgespeichert werden und wem diese Informationen zur Verfügung gestellt werden.

Darüber hinaus werden Zertifizierungskonzepte für Energieversorger entwickelt. Dafür werden speziell an die Bedürfnisse kleiner und mittlerer Energieversorger angepasste Prüfkriterien, Checklisten und Guidelines erarbeitet, um eine kosteneffiziente Zertifizierung gemäß gültiger Standards und gesetzlicher Vorgaben zu ermöglichen. Mit einer solchen Zertifizierung sollen Energieversorger dem Gesetzgeber, aber auch ihren Endkunden und Geschäftspartnern gegenüber, die Einhaltung eines hohen Sicherheitsniveaus nachweisen können. Gleichzeitig wäre dies ein Beitrag zur Erhöhung der Markttransparenz für Endkunden.

Es soll ein Anforderungskatalog auf Basis der entwickelten Metriken konzipiert werden, der es erlaubt, eine möglichst vollständige Auflistung wichtiger Anforderungen zu identifizieren, die benötigt werden, um eine Zertifizierungsaussage treffen zu können. Dieser orientiert sich an zuvor ausgearbeiteten relevanten Prüfkriterien, die im Rahmen einer Zertifizierung zu prüfen sind. Die Herausforderung bei der Erstellung eines solchen Prüfkatalogs besteht im Ausarbeiten eindeutiger und möglichst objektiv zu bewertender Prüffragen. Bei der Ausarbeitung des Prüfkatalogs sollen auch bestehende relevante Zertifizierungen berücksichtigt werden. Die Berücksichtigung bestehender Zertifizierungen verfolgt das Ziel, die Kosten für die weitere Zertifizierung zu minimieren. Hierzu muss die Abdeckung der Prüfpunkte von vorhandenen Zertifizierungen analysiert werden. Je nach Abdeckungsgrad der Anforderungen können zu prüfende Punkte aus einer bestehenden Zertifizierung abgeleitet werden und somit der Prüfumfang verringert werden.

4 Methodisches Vorgehen

Das Forschungsvorhaben sieht eine praxisnahe Forschungsmethodik bestehend aus (1) einer Analyse der Arbeitspraxis, (2) der Entwicklung von Konzepten und Softwarewerkzeugen und (3) deren Evaluation in der Praxis vor (Wulf et al. 2015). Ziel der ersten Phase ist es, mittels qualitativer und quantitativer empirischer Forschungsmethoden die derzeitige Arbeits- und Kooperationspraxis bei Energieversorgern hinsichtlich systemsicherheitsrelevanter Prozesse zu untersuchen, um Anforderungen an mögliche Konzepte und Werkzeuge zur Unterstützung dieser Praxis zu erhalten. Dazu werden verschiedenen Studien bei assoziierten Energieversorgern vor Ort im Rahmen von Interviews, Workshops, Beobachtungen und Dokumentenanalysen durchgeführt. Außerdem wird gemeinsam mit einem deutschlandweit agierendem Stadtwerkenetzwerk ein regelmäßig stattfindender Arbeitskreis zum Thema IT-Sicherheit für Energieversorger gebildet, der den bilateralen Austausch und die Kooperation zwischen dem Projektkonsortium und interessierten Stadtwerken ermöglichen soll.

Bei der Entwicklung der Konzepte und Werkzeuge verfolgen wir einen partizipativen und iterativen Ansatz. Die Grundlage hierfür bilden die Ergebnisse der Praxisanalyse sowie relevante rechtliche und regulatorische Rahmenbedingungen. Die (Zwischen-)Ergebnisse werden in regelmäßigen Abständen im Rahmen von Workshops, Fokusgruppen sowie dem erwähnten Arbeitskreis mit Anwendern diskutiert, validiert und weiterentwickelt.

Ein wesentliches Ziel ist es, die Konzepte und Werkzeug-Demonstratoren so zu gestalten und zu entwickeln, dass diese im Rahmen des Forschungsprojekts im Anwendungsfeld unter realen Bedingungen evaluiert und auf ihre Praxistauglichkeit hin untersucht werden können.

5 Zusammenfassung

In dieser Arbeit wurde aufgezeigt, dass kleine und mittlere Energieversorger sowohl den Schutz als auch insbesondere die Wirtschaftlichkeit ihrer Infrastrukturen sicherstellen müssen. Dabei sind die Energieversorger zur Umsetzung und Einhaltung vorgegebener Mindeststandards durch die Vorgaben des IT-Sicherheitsgesetzes verpflichtet. Das Projekt hat zum Ziel, die Energieversorger dabei zu unterstützen, insbesondere in drei übergeordneten Kernthemen: der Bewertung von IT-Sicherheit, Wissensaustausch zwischen und Zertifizierung der Energieversorger. Die Erfassung der Anforderungen, die Entwicklung der Konzepte und Demonstratoren sollen dabei in enger Kooperation mit den assoziierten Partnern, kleinen und mittelgroßen Energieunternehmen, als

iterativer Prozess durchgeführt werden. Besonderes Augenmerk liegt dabei auch auf der Zukunftsfähigkeit der entwickelten Konzepte, das heißt diese sollen möglichst leicht an neue Technologien angepasst werden können.

6 Förderhinweis

Die Forschungsarbeiten werden durch das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen“ gefördert.

7 Literatur

BDEW (2015) Marktteilnehmer Energie aktuell - Vielfalt im Energiemarkt. https://www.bdew.de/internet.nsf/id/5512898B85FDC9C1C12579C2004225A8/$file/Marktteilnehmer%20Energie%20aktuell_online_o_halbjaehrlich_Ki_10042015.pdf. Abgerufen am 18.09.2015

BNetzA (2011) „Smart Grid“ und „Smart Market“ - Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems.

Fischer-Hübner S, Grimm R, Lo I, Möller S, Müller G, Volkamer M (2011) Gebrauchstaugliche Informationssicherheit. Die Zeitschrift für Informationssicherheit Jg. 2011 (4):14-19

Grefe C (2014) „Blackout“. In: Die Zeit, Nr. 16/2014

Herzog A (2007) Usable Security Policies for Runtime Environments. *Linköping Studies in Science and Technology*. PhD Thesis, Department of Computer and Information Science, Linköping University

ISO/IEC 27001 (2015) IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

ISO/IEC 27002 (2008) IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management

Parkin S, van Moorsel A, Ingelsant P (2010) A stealth approach to usable security: helping IT security managers to identify workable security solutions. In: Workshop on New Security Paradigmns (NSPW ´10). 33-50.

PwC (2014) 14th PwC Global Power & Utilities Survey: "A different energy future -- Where energy transformation is leading us". PricewaterhouseCoopers International Limited.

Pfleeger SL, Cunningham RK, “Why Measuring Security is hard”. IEEE Security & Privacy 8(4):46-54

Whitten A, Tygar, JD (1999) Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th conference on USENIX Security Symposium.

Wulf V, Müller C, Pipek V, Randall D, Rohde M, Stevens G (2015) Practice-based Computing: Empirically-grounded Conceptualizations derived from Design Case Studies. In: Wulf V, Schmidt K, Randall D (Hrsg.) Designing Socially Embedded Technologies in the Real-World, Springer, London, 111-150