Beschreibung eines prüffragengetriebenen Mehrbenutzersystems zur Durchführung von Sicherheitsüberprüfungen

Hannes Federrath, Dominik Herrmann, Christoph Gerber
Lst. Management der Informationssicherheit, Universität Regensburg
[vorname.nachname]@wiwi.uni-regensburg.de

Arbeitsbericht, Universität Regensburg, 2011

In diesem Arbeitspapier wird der Prototyp eines Softwarewerkzeuges beschrieben, mit dem auf Basis von Prüffragen aus den BSI-Grundschutzkatalogen ein Untersuchungsgegenstand begutachtet werden kann. Dieses Werkzeug unterstützt Arbeitsgruppen bei der Durchführung von Audits und Revisionen und kann auch zur Durchführung einer Selbstdokumentation eingesetzt werden. Mögliche Erweiterungen, insbesondere in den Bereichen der Einbindung externer (Vertrags-)Partner und der Auswertung von Benutzerinteraktionsdaten zur Verbesserung des Werkzeuges werden aufgezeigt.

1 IT-Sicherheitsmanagement und IT-Sicherheitsüberprüfungen

IT-Sicherheitsmanagement umfasst das planhafte Absichern und Aufrechterhalten der IT-Infrastruktur einer Organisation oder eines Unternehmens gegen sowohl beabsichtigte als auch unbeabsichtigte Störungen der innerbetrieblichen Abläufe. Berücksichtigt werden dabei stets die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der IT-Sicherheit. Die wesentlichen Aufgaben des IT-Sicherheitsmanagements sind neben der Entwicklung einer Sicherheitspolitik und eines Sicherheitskonzeptes, der Realisierung von Sicherheitsmaßnahmen sowie Schulung und Sensibilisierung von Mitarbeitern auch die Erhaltung der IT-Sicherheit im laufenden Betrieb. Dabei ist IT-Sicherheitsmanagement als kontinuierlicher Prozess zu begreifen, der dazu dienen soll, die IT-Sicherheit innerhalb einer Organisation zu gewährleisten (vgl. [HS10, S. 290f.], [SW07, S. 489f.], [Bun08a, S. 82]).

Mit dem BSI-Standard 100-2 [Bun08a], in Verbindung mit den Grundschutzkatalogen [Bun09], gibt das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* Unternehmen und Behörden ein strukturiertes Vorgehensmodell an die Hand, mit dem sich die IT-Sicherheit von Unternehmen gezielt überprüfen und verbessern lässt. Das erreichte Sicherheitsniveau kann ein Unternehmen nach erfolgreicher Zertifizierung (z. B. ISO 27001-Zertifizierung) auch nach außen kommunizieren.

Teil dieses BSI-Sicherheitsprozesses ist dabei auch das regelmäßige Überprüfen der Wirksamkeit von getroffenen Sicherheitsmaßnahmen und eine Verbesserung der Absicherung des Unternehmens.

1.1 Einsatzgebiete des Prüfwerkzeuges

Besonders im Bereich der Erhaltung der IT-Sicherheit im laufenden Betrieb besteht Anwendungspotenzial für das hier beschriebene prüffragengetriebene Werkzeug, um den Prozess der Begutachtung eines Untersuchungsgegenstandes zu begleiten. Sicherheitsüberprüfungen im Bereich von *Informationssicherheits-Managementsystemen* (ISMS) finden häufig in Form von Revisionen [Bun10] und Audits [Bun08b] statt. Doch auch im Bereich der Entwicklung eines Sicherheitskonzeptes unter der Verwendung eines Soll-/Ist-Vergleiches [Bun08a, S. 68] kann das in diesem Arbeitspapier beschriebene Werkzeug unterstützenden Charakter in Form der Durchführung einer ersten Selbstdokumentation aufweisen. Die in den BSI-Grundschutzkatalogen [Bun09] enthaltenen Prüf- und Kontrollfragen eignen sich dabei als Datengrundlage.

1.2 Zugrundeliegende Funktionsweise

Das Werkzeug orientiert sich bei der hierarchischen Anordnung von Prüffragen zum einen an der Anordnung aus den BSI-Grundschutzkatalogen und zum anderen an der Anordnung nach Control Areas, entnommen aus dem Standard ISO 27001/2. Für Letztere stellt das BSI eine eigene Zuordnungstabelle [Bun] bereit. Das browserbasierte Prüffragenwerkzeug präsentiert dem Sachbearbeiter eine Liste von Prüffragen, die er nun entweder sukzessive oder auch in beliebiger Reihenfolge abarbeiten kann. Durch die browserbasierte Lösung können auch mehrere Personen gemeinsam an der Abarbeitung der Prüfliste arbeiten.

1.3 Mehrbenutzerfähigkeit

Interne Kollaboration

Sicherheitsmanagement ist nur selten eine 1-Personen-Aufgabe. Viel mehr ist IT-Sicherheit als Querschnittsaufgabe zu betrachten, die alle Teilbereiche eines Unternehmens betrifft. Bei der Erhebung des Ist-Zustandes der IT-Infrastruktur beispielsweise sind in der Regel mehrere Personen, jeweils aus dem entsprechenden Fachbereich beteiligt. Hier ist es wünschenswert, dass Mitarbeiter des gleichen Unternehmens durch ein mehrbenutzerfähiges Werkzeug in die Lage versetzt werden, gemeinsam sicherheitsrelevante Fragestellungen zu bearbeiten. Auch im Bereich von Audits und Revisionen kann ein gemeinsames Prüffragenwerkzeug helfen, Medienbrüche zu vermeiden und den notwendigen Kommunikationsaufwand reduzieren.

Semiexterne Kollaboration

Nicht nur Arbeitsabläufe innerhalb eines Unternehmens können durch geeignete Softwarewerkzeuge unterstützt werden. Denkbar ist außerdem die Etablierung von Schnittstellen hin zu semiexternen Kooperationspartnern, also in der Regel Partnern, die nicht zum Unternehmen gehören, mit denen aber eine vertragliche Beziehung besteht. Im Rahmen des IT-Sicherheitsmanagements können dies vor allem externe Beratungsunternehmen oder auch Auditoren sein, die hier in den Bearbeitungsprozess mit eingebunden werden.

Externe Kollaboration

Derzeit stellen Beraterfirmen die einzig etablierte Möglichkeit dar, unternehmensübergreifend Daten zum Sicherheitsmanagement zu sammeln und im Rahmen der eigenen erworbenen Erfahrung wieder einzusetzen. Diskussionsforen zum Thema Grundschutz und zur

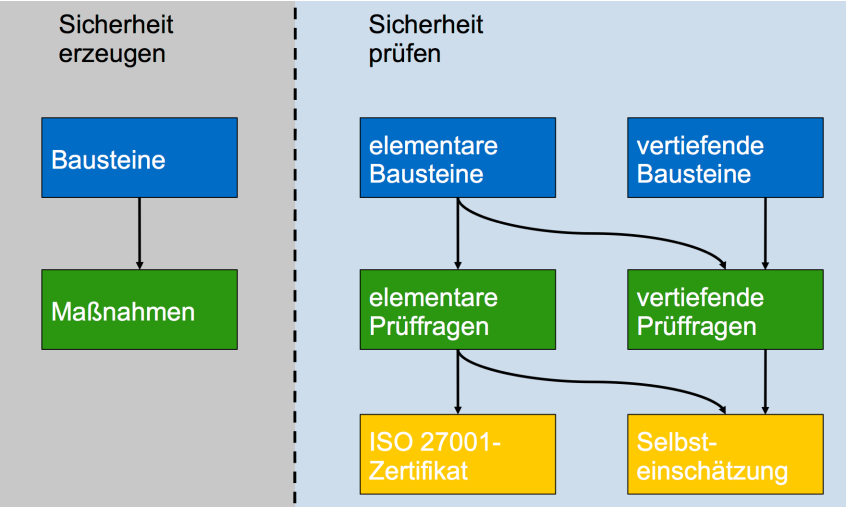

Abbildung 1: Geplante Umstrukturierung der BSI-Grundschutzkataloge nach [Isa10].

gezielten Auswahl und Anwendung von einzelnen Maßnahmen oder dem Begegnen von Gefährdungen gibt es bisher nicht oder kaum. Die Erweiterung des prüffragengetriebenen IT-Sicherheistmanagementwerkzeuges zum Datenaustausch über Unternehmensgrenzen bietet Beteiligten viele Vorteile. So kann es dadurch z. B. möglich werden, sich mit anderen Unternehmen hinsichtlich spezieller Key Performance Indikatoren (KPIs) zu vergleichen oder es können gezielt Diskussionen bezüglich der Umsetzung einzelner Maßnahmen angestellt werden. Hier sind zahlreiche Erweiterungen denkbar, von denen einige in den Abschnitten 3.2 und 3.3 angesprochen werden.

Das im Rahmen dieses Arbeitsberichts erstellte Prüffragenwerkzeug unterstützt zum jetzigen Zeitpunkt hauptsächlich Funktionen zur internen Kollaboration.

1.4 Neuerungen im BSI-Grundschutz

Mit der geplanten Umstrukturierung des BSI-Grundschutzes in der 12. Ergänzungslieferung bekommen die in den Grundschutzkatalogen hinterlegten Prüffragen ein größeres Gewicht und lösen damit die nicht immer inhaltlich vollständigen Kontrollfragen mehr und mehr ab. Der Anspruch an die Prüffragen ist dabei, dass sie Ziel und Grundrichtung einer Maßnahme vorgeben und in ihrer Gesamtheit als letzte Checkliste verwendet werden können, um die Wirksamkeit der Absicherung von Unternehmensbereichen in Audits und Revisionen zu überprüfen [Isa10]. Aus Gründen der Komplexitätsreduktion sollen in künftigen Versionen der BSI-Grundschutzkataloge Bausteine hinsichtlich ihrer Relevanz unterschieden werden. Das sog. *E-V-Modell* sieht eine Unterscheidung in die Gruppen *elementare Bausteine* und *vertiefende Bausteine* (vgl. Abbildung 1) vor. Die Bewertung und Umsetzung von Maßnahmen, die in elementaren Bausteinen aufgeführt sind, ist notwendiger Bestandteil zum Erreichen einer ISO 27001-Zertifizierung nach diesem Modell. Vertiefende Bausteine tragen speziellen Unternehmenskonfigurationen Rechnung und werden so lediglich bewertet, umgesetzt und geprüft, wenn die entsprechenden Lösungen auch im Unternehmen eingesetzt oder benötigt werden [Isa10].

Bereits zum jetzigen Zeitpunkt der 11. Ergänzungslieferung sind die BSI-Grundschutzkataloge eine gute Quelle für Prüffragen. So gibt es bereits ca. 1100 Prüffragen verteilt auf 278 Maßnah-

Abbildung 2: Ausprägungen von Prüffragen.

men. Spitzenreiter hierbei ist die Maßnahme *M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen* für die insgesamt 17 Prüffragen hinterlegt sind. Ergänzend dazu kann man auf etwa 1800 Kontrollfragen zugreifen, die sich auf 700 Maßnahmen verteilen.

2 Funktionsbeschreibung des kollaborativen Prüffragensystems

Mit dem derzeitig vorliegenden System ist es einfach möglich, anhand der Beantwortung von Prüffragen das erreichte Sicherheitsniveau eines Untersuchungsgegenstandes (beispielsweise ein ISMS) zu begutachten. Am Begutachtungsprozess selbst können dabei mehrere Personen (auch gleichzeitig) teilnehmen.

2.1 Aufbau und Verwaltung von Prüffragen

Die Grundlage des Prüffragenwerkzeuges bilden die, aus den BSI-Grundschutzkatalogen entnommenen Prüf- und Kontrollfragen. Diese werden entsprechend der, in der ISO-Norm 27001/2 spezifizierten Control-Areas angeordnet und dargestellt.

Eine Prüffrage besteht prinzipiell aus drei Teilen (vgl. Abbildung 2). Im *Teilbereich 1* einer Prüffrage wird zuerst der aktuelle Befund (Status quo) erfasst und optional eine Empfehlung zur Verbesserung ausgesprochen. Die Elemente *Quelle* und *Verweis* dienen dabei als Zeiger auf den Untersuchungsgegenstand. Im *Teilbereich 2* werden die Kriterien *Relevanz*, *Bewertung* und *Kritikalität* erfasst. Es wird die Wichtigkeit der Prüffrage im Bezug auf den Untersuchungsgegenstand abgebildet und es wird die Wirksamkeit der Maßnahme bewertet. Diese Daten werden jeweils mit mehreren Ausprägungen auf einer ordinalen Skala erfasst (für das Kriterium *Relevanz* beispielsweise sind die Stufen *sehr relevant*, *normal* und *weniger relevant* vorgesehen) und können ebenfalls für statistische Aussagen über den Untersuchungsgegenstand herangezogen werden (vgl. Abschnitt 2.3). *Teilbereich 3* zeigt bereits Ansätze der Integration von semi-externen Teilnehmern. Hier wird einer dritten Partei die Möglichkeit gegeben, sich zu dem Befund zu äußern. Abgebildet ist ferner, dass auf die Stellungnahme seitens des Gutachters noch einmal reagiert werden kann.

Nicht immer wird eine Prüffrage durch einen Sachbearbeiter sofort und abschließend bearbeitet. Durch Setzen des Indikators *Final* werden diejenigen Prüffragen markiert, die nach Meinung des Bearbeiters erschöpfend beantwortet wurden. Herrscht bei einer Frage Unklarheit vor, kann

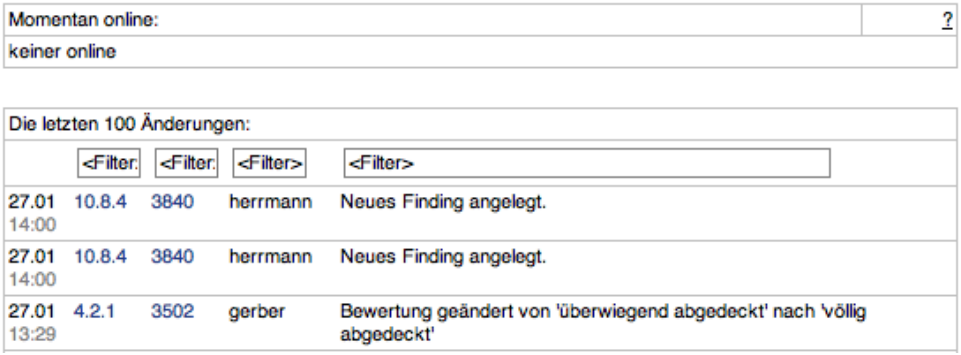

Abbildung 3: Änderungshistorie bearbeiteter Prüffragen.

ein Bearbeiter den Indikator *Diskussionsbedarf* setzen, und damit vormerken, dass bei einer Prüffrage weitere Informationen benötigt werden.

Der in dem Prüffragenwerkzeug hinterlegte Fragenkatalog ist nicht auf die Prüf- und Kontrollfragen aus den BSI-Grundschutzkatalogen beschränkt. Er kann leicht um eigene Fragen erweitert werden, bzw. können nicht benötigte Fragen ausgeblendet werden. Auch das Erstellen und Laden eigener Kataloge ist technisch möglich.

Durch die Verwendung der Ajax-Technologie [SW07, S. 433] muss die zentrale Prüffragenliste beim Eintragen von Informationen nicht jedes Mal neu geladen werden, was den Bearbeitungskomfort enorm erhöht.

2.2 Änderungshistorie und Mehrbenutzerfähigkeit

Änderungen auf Ebene der einzelnen Prüffragen, wie z. B. das Ergänzen des Befundtextes oder das Ändern des Abdeckungskriteriums werden in einer sog. *Änderungshistorie* (vgl. Abbildung 3) erfasst. Diese Funktion erhöht insgesamt die Transparenz beim Bearbeitungsvorgang und mögliche Fehler können erkannt und leicht korrigiert werden. Die Änderungsliste ist dabei so ausgelegt, dass die aufgelisteten Eingaben hinsichtlich der Kriterien *Control-Area*, *Prüffragen-ID*, *Sachbearbeiter* und *Änderung* gefiltert werden können. Die Änderungshistorie eignet sich als Datenquelle für eine Vielzahl möglicher statistischer Auswertungen rund um die Arbeitsweisen im Zusammenhang mit dem BSI-Grundschutz (vgl. Abschnitt 3.3).

Ebenfalls in Abbildung 3 ersichtlich ist der Benutzerindikator, eine Funktion, die anzeigt, welche weiteren Sachbearbeiter ebenfalls zurzeit mit den Prüffragen arbeiten. In Verbindung mit der Änderungshistorie sieht man ferner, mit welchem Teil des Fragenkatalogs sich der Bearbeiter gerade beschäftigt. Dies ermöglicht es leichter Rücksprachen mit anderen Sachbearbeitern zu treffen zu einem Zeitpunkt, zu dem sie selbst gerade auch mit der Materie beschäftigt sind und ermöglicht so eine effizientere Arbeitsweise.

2.3 Statistische Funktionen und Exportfunktionalität

Derzeit sind in dem Prüffragenwerkzeug zwei Formen der statistischen Auswertung implementiert. Zum einen ist es Benutzern möglich, für die einzelnen Teilereiche aus ISO 27001/2 tabellarisch einzusehen, wie viele Prüffragen hierzu hinterlegt sind und der anteilige Abdeckungsgrad in Relation zum maximal möglichen Abdeckungsgrad wird visualisiert.

Auf einer höheren Aggregationsebene sind Findinganzahl, Relevanz und Abdeckung für die einzelnen Control-Areas tabellarisch und in Form eines Kiviat-Graphen dargestellt und geben

Auswertungen

Relevanz: sehr relevant: 101 normal: 359 weniger relevant: 89
Abdeckung: völlig abgedeckt: 1 überwiegend abgedeckt: teilweise abgedeckt: 125 gar nicht abgedeckt: 150

Bereich	Findinganzahl	Relevanz	Abdeckung
ISMS	43	2.19	0.30
RESP	3	2.00	0.00
AUDIT	5	2.00	0.40
REVIEW	4	1.00	0.00
IMPROVE	4	2.00	1.00
COMGMT	130	1.98	0.16
ACCESS	111	1.91	0.10
ISADM	63	2.10	0.29
ISIM	15	2.40	0.00
BCM	19	2.58	0.42
COMPL	21	2.05	0.19
POLICY	6	1.83	0.67
ORGIS	53	1.92	0.43
ASSETM	17	2.35	0.24
HR	16	2.00	0.31
PHYS	39	1.90	0.28

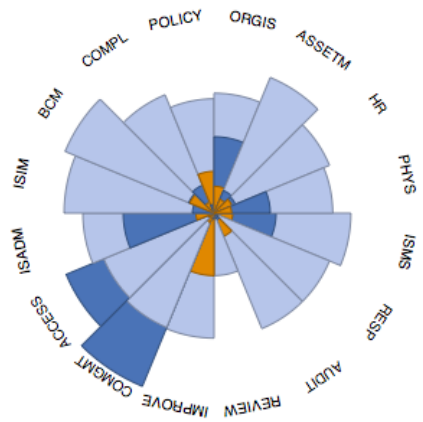

Abbildung 4: Statistische Auswerung von Prüffragen auf Basis der Bereiche des Untersuchungsgegenstandes.

so schnell Überblick über die Ergebnisse der Sicherheitsbetrachtung (vgl. Abbildung 4).

Zu Dokumentationszwecken ist es möglich, den Datenbestand aus dem Prüffragenwerkzeug zu exportieren und mit anderen Anwendungen weiterzuverarbeiten. Umgesetzt ist derzeit ein Datenexport für Microsoft Excel sowie LaTeX.

3 Erweiterungsaspekte

3.1 Entwicklung von Workflow-Schnittstellen zur semi-externen Kollaboration

Bisher ist das Prüffragenwerkzeug optimiert für die Arbeitsweise von kleinen internen Gruppen (vgl. Abschnitt 1.3). Obwohl bereits erste Ansätze existieren, semi-externe Benutzer in den Bearbeitungsprozess einzubinden, besteht hier noch erhebliches Erweiterungs- und Verbesserungspotenzial. So müssen typische Formen der Zusammenarbeit von internen Sachbearbeitern und Beratungsunternehmen oder Auditoren untersucht werden und Phasenmodelle, Schnittstellen und Berechtigungsschemata gefunden und implementiert werden, die helfen, die Zusammenarbeit an Themen zum Sicherheitsmanagement weiter zu verbessern.

3.2 Unternehmensübergreifende Funktionen (externe Kollaboration)

Denkbar ist eine Erweiterung des Prüffragenwerkzeuges zur Anbindung mehrerer externer Parteien. Eine solche Erweiterung würde die Grundlage schaffen, sich mit anderen Unternehmen hinsichtlich noch zu identifizierender Kennzahlen wie z. B. der Abdeckung pro Bereich oder auch der getätigten Sicherheitsinvestitionen zu vergleichen. Diese Erweiterung könnte zentral auf einem Server laufen, auf dem mehrere Instanzen des Prüffragenwerkzeuges für die entsprechenden Arbeitsgruppen gestartet werden. Da es sich bei den erhobenen Daten jedoch um Informationen handelt, die den Sicherheitsstatus eines Unternehmens dokumentieren und daher ein erhöhter Schutzbedarf vorliegt, müssen hier Lösungen zum mehrseitig sicheren Informationsaustausch [RPM96] gefunden werden. Möglich in diesem Zusammenhang ist, dass jedes Unternehmen eine eigene Instanz des erweiterten Prüffragenwerkzeuges in

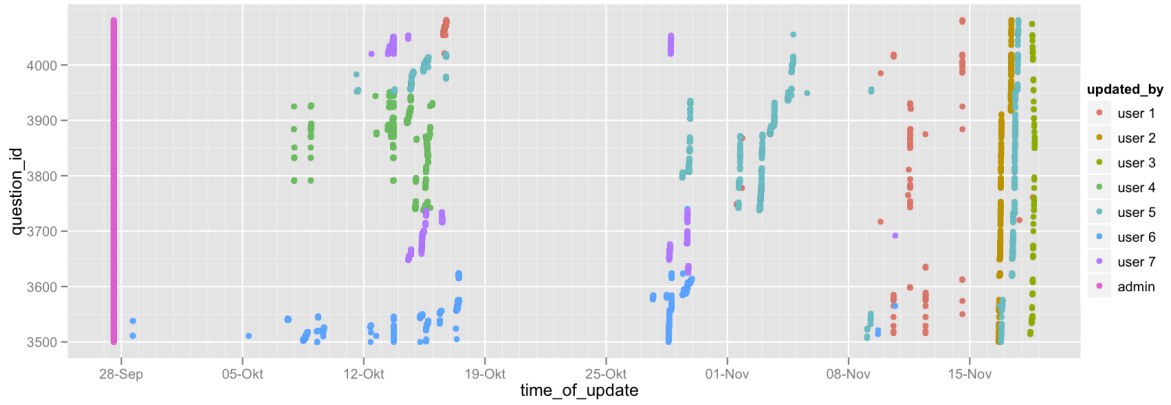

Abbildung 5: Auswertung eines kollaborativ Erarbeiteten Untersuchungsgegnstand.

seinem Schutzbereich betreibt und entsprechende Kennzahlen sicher, unter Zuhilfenahme einer zentralen Instanz berechnet werden. Vorarbeiten hierzu existieren bereits (vgl. [HSF+09]).

3.3 Strukturanalysen und -bildung von Prüffragen

Auf Basis der Daten der Änderungshistorie lassen sich gängige Arbeitsweisen bei der Bearbeitung der Prüffragen erkennen. In Abbildung 5 sieht man beispielsweise, dass sich einige Benutzer besonders auf spezielle Teilbereiche des Prüffragenkataloges konzentrieren. Durch die Analyse solcher Nutzungsdaten soll es in Zukunft möglich werden, die Prüffragen für Sachbearbeiter in Abhängigkeit seines speziellen Bearbeitungsprofiles zu gruppieren und ihnen auf diese Weise die Arbeit mit dem Werkzeug zu erleichtern. Bekommt man die Möglichkeit, die Änderungshistorie von mehreren Arbeitsgruppen zu analysieren, würden sich daraus eventuell allgemeingültige Wechselwirkungen identifizieren lassen (beispielsweise: Sachbearbeiter, die sich um den Virenschutz kümmern, übernehmen in der Regel auch die Prüfung der Firewalllösung) und so eine Neustrukturierung des Fragenkataloges ermöglichen, die ergonomischere Arbeitsweisen begünstigt.

Auch weitere Analysen bezüglich der Zusammenarbeit von Gruppen können sich auf Basis der Änderungshistorie untersuchen lassen (beispielsweise das gegenseitige Korrekturlesen von Antworten) und helfen, den Workflow für arbeitsgruppenbasierte Sicherheitsüberprüfungen zu verbessern.

Literatur

[Bun] Bundesamt für Sicherheit in der Informationstechnik. Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz.

[Bun08a] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, 2008.

[Bun08b] Bundesamt für Sicherheit in der Informationstechnik. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits, 2008.

[Bun09] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Kataloge 11. Ergänzungslieferung, 2009.

[Bun10] Bundesamt für Sicherheit in der Informationstechnik. Informationssicherheitsrevision – Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz, März 2010.

[HS10] Jürgen Hofmann and Werner Schmidt. *Masterkurs IT-Management*. 2., aktualisierte und erweiterte Auflage. Vieweg Verlag, Wiesbaden, 2010.

[HSF+09] Dominik Herrmann, Florian Scheuer, Philipp Feustel, Thomas Nowey, and Hannes Federrath. A privacy-preserving platform for user-centric quantitative benchmarking. In Simone Fischer-Hübner, Costas Lambrinoudakis, and Günther Pernul, editors, *Trust, privacy and security in digital business: 6th international conference, TrustBus 2009, Linz, Austria, September 3 - 4, 2009; proceedings*, volume 5695 of *Lecture Notes in Computer Science*, pages 32–41. Springer, Berlin, Heidelberg, 2009.

[Isa10] Isabel Münch. Aktuelle Entwicklungen im IT-Grundschutz. IT-Grundschutz-Tag, Oktober 2010.

[RPM96] K. Rannenberg, A. Pfitzmann, and G. Müller. Sicherheit, insbesondere mehrseitige IT-Sicherheit. *Informationstechnik und technische Informatik*, 38:7–10, 1996.

[SW07] Uwe Schneider and Dieter Werner. *Taschenbuch der Informatik*. 6. neu bearbeitete Auflage. Hanser Verlag, München, 2007.