Kollaboratives IT-Sicherheitsmanagement auf Basis von BSI-Grundschutz

Hannes Federrath, Christoph Gerber

{federrath, gerber}@informatik.uni-hamburg.de

Abstract: Kollaboratives IT-Sicherheitsmanagement beschreibt Möglichkeiten der gegenseitigen Unterstützung von Unternehmen bei der Implementierung und Aufrechterhaltung des IT-Sicherheitsmanagementprozesses mittels überbetrieblichem Informationsaustausch. Dabei wird ausgehend von der Annahme, dass sich durch interorganisatorische Zusammenarbeit bessere Entscheidungen für die Umsetzung von IT-Sicherheitsmaßnahmen treffen lassen, ein System beschrieben, das die Vorgehensweise nach BSI-Grundschutz mittels einer technischen Lösung um einen unternehmensübergreifenden Datenaustausch erweitern soll.

1 Einführung

Unternehmen, die ihre Infrastruktur nach einer Standardvorgehensweise gegen Gefährdungen der Informationssicherheit absichern, sind neben dem Schutz des Unternehmens auch daran interessiert, ökonomische Sicherheitsinvestitionen zu tätigen [Fed06]. Laut [KWD+10] greift zur Umsetzung nur etwa die Hälfte aller Unternehmen auf die Hilfe externer Dienstleister zur Beratung zurück. Da auf IT-Sicherheitsmanagement spezialisierte Beratungsunternehmen mehr als nur einen Kunden bei der Realisierung von Informationssicherheitsmanagementsystemen (ISMS) betreuen, können sie in der Regel auf einen breiten Erfahrungsschatz bei der Umsetzung sowie bei der Schätzung von Aufwänden zurückgreifen. Die zweite Gruppe von Unternehmen, die Sicherheitsmanagement im Alleingang betreibt, hat zunächst keine Möglichkeit, vergleichsbasiert Entscheidungen über IT-Sicherheitsinvestitionen zu treffen.

Mit diesem Beitrag wird ein Informationssystem skizziert, das es ermöglichen soll, unternehmensübergreifend Daten zum IT-Sicherheitsmanagement auszutauschen und zur Entscheidungsfindung heranzuziehen. Ein solches System soll dabei nicht als Alternative zu klassischen Beratungsleistungen im IT-Sicherheitsbereich gesehen werden, sondern als Ergänzung hierzu, da auch Beratungsunternehmen von einer breiteren Basis an Vergleichsdaten profitieren können.

Als Ausgangspunkt dient die im deutschsprachigen Raum vielfach verwendete Vorgehensweise zur Unternehmensabsicherung nach IT-Grundschutz, welche vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird (vgl. [HS10, S. 298]). Das BSI bietet derzeit insgesamt vier Standards (BSI 100-1 bis BSI 100-4: [Bun08a, Bun08b, Bun08c, Bun08d]) an, in denen die *Einführung eines ISMS*, die *Vor-*

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

gehensweise nach BSI-Grundschutz, eine *Vorgehensweise zum Risikomanagement* sowie ein *Vorgehen zum Notfallmanagement* beschrieben sind. Durch die Modellierung eines Informationsverbundes mittels BSI-Grundschutz wird zum einen die Komplexität des Untersuchungsgegenstandes beherrschbar [Bun09b], zum anderen bietet die Vorgehensweise eine Vielzahl von Anknüpfungspunkten für einen unternehmensübergreifenden Datenaustausch.

2 Die Grundidee des kollaborativen IT-Sicherheitsmanagements

In Abbildung 1 ist der schematische Aufbau für eine Infrastruktur zum kollaborativen Sicherheitsmanagement abgebildet. Vorgeschlagen wird eine Client-Server-Architektur, bei der mehrere Unternehmen lokal Daten zur Arbeit mit dem Vorgehensmodell nach BSI-Grundschutz [Bun08b] sammeln und einer zentralen Komponente zur Verfügung stellen.

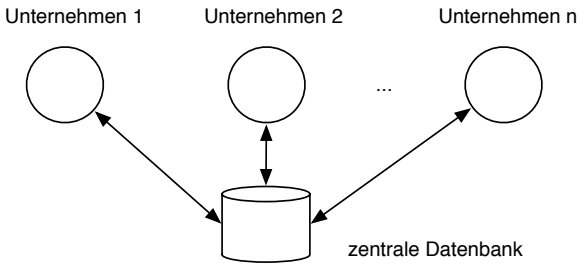

Abbildung 1: Schematische Abbildung des interorganisatorischen Informationsaustauschs im IT-Sicherheitsmanagement

2.1 Datenquellen in der Vorgehensweise nach BSI-Grundschutz

Abbildung 2 zeigt, wie die Teilkataloge des BSI-Grundschutzes im Unternehmenskontext Verwendung finden. Ein Unternehmen besitzt mehrere schützenswerte Unternehmenswerte (Assets). Diese Assets werden im Rahmen einer *Strukturanalyse* auf sogenannte *Bausteine* abgebildet. Daran schließt sich eine *Schutzbedarfsfeststellung* an, bei der die für die Bausteine notwendigen *Schutzbedarfsniveaus* hinsichtlich der drei Schutzziele *Vertraulichkeit, Integrität* und *Verfügbarkeit* ermittelt werden. Für jeden Baustein ist in den Grundschutzkatalogen [Bun09a] eine Menge von *Gefährdungen* hinterlegt, die auf das Asset ein-

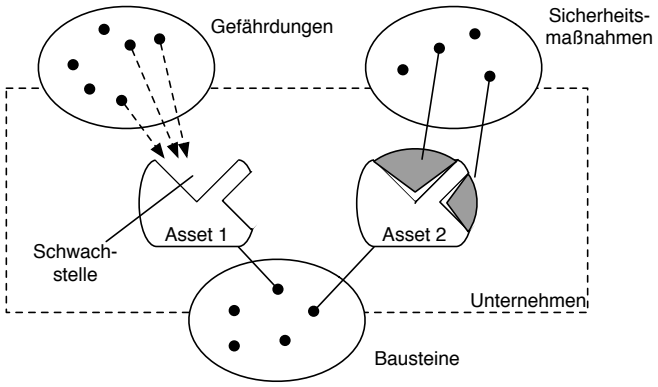

Abbildung 2: Die Zuordnung von Elementen aus den Grundschutzkatalogen zu Unternehmenswerten in Anlehnung an [Now11, S. 19].

wirken sowie eine Menge von *Maßnahmen* die getroffen werden können, um den entsprechenden Baustein abzusichern. Im *Basis-Sicherheitscheck* wird mittels Soll-Ist-Vergleich ein Delta an Maßnahmen zwischen den vom BSI vorgeschlagenen und dem tatsächlichen Zustand ermittelt und daraus ein *Realisierungsplan* zur Absicherung des IT-Verbundes abgeleitet. Optional wird für Bausteine mit erhöhtem Schutzbedarf eine *ergänzende Risikoanalyse* durchgeführt, bei der mittels *Gefährdungsanalyse* weitere geeignete Sicherheitsmaßnahmen für einen Baustein identifiziert und dem Realisierungsplan hinzugefügt werden. Nach einer *Konsolidierung* des Realisierungsplanes erfolgt die eigentliche *Umsetzung* der Maßnahmen. Durch regelmäßige *Revisionen* wird für die *Erhaltung* der IT-Sicherheit im laufenden Betrieb gesorgt. Diesem wiederholt ablaufenden Prozess geht initial die Vorbereitung zur Einführung eines ISMS seitens der Unternehmensleitung voraus.

Tabelle 1 zeigt, welche Datenquellen innerhalb der Vorgehensweise nach BSI-Grundschutz zu einem unternehmensübergreifenden Datenaustausch prinzipiell herangezogen werden können. Gerade zur Auswertung von Reihenfolgen, beispielsweise bei der Einstufung von Maßnahmen im Rahmen der Ist-Erhebung oder der Abarbeitung von Maßnahmen im Realisierungsplan ist es wichtig, zu jeder Systemeingabe auch immer einen Zeitstempel mitzuerheben (ggf. in Bezug zu einem relativen Anfangszeitpunkt). Hierdurch lässt sich bei einer späteren Datenanalyse die Bearbeitungsreihenfolge rekonstruieren.

2.2 Vorteile des kollaborativen IT-Sicherheitsmanagements

Die Grundannahme beim unternehmensübergreifenden IT-Sicherheitsmanagement ist, dass Unternehmen von den Erfahrungen anderer Unternehmen bezüglich der Arbeit im Sicherheitsmanagementbereich profitieren können. Im Rahmen von Initiativen wie dem *Netzwerk für Informationssicherheit im Mittelstand* (NIM) des Regensburger IT-Speichers

Tabelle 1: Relevante Datenquellen für den unternehmensübergreifenden Austausch

Bereich	Datenquelle
Allgemeine Faktoren	- Branche - Unternehmensgröße - Grad der IT-Abhängigkeit - Niveau der Informationssicherheit im Unternehmen (vgl. [Now11, S. 154f.])
Strukturanalyse	- ausgewählte Bausteine des IT-Verbundes
Schutzbedarfsfeststellung	- Schutzbedarfe für Bausteine
Grundschutzanalyse	- Bausteinen zugehörige Maßnahmen mit Siegelstufen - Umsetzungsgrad der Maßnahmen (Ist-Zustand) - Begründung der Einstufung des Umsetzungsgrades
Ergänzende Risikoanalyse	- ausgewählte Bausteine - Auswahl relevanter Gefährdungen für Bausteine
Realisierungsplan und Umsetzung	- geplante und tatsächliche Kosten je Maßnahme - geplanter und tatsächlicher Personalaufwand je Maßnahme
Aufrechterhaltung	- Bausteine mit Verbesserungspotential - Maßnahmen mit Nachbesserungspotential

sollen Aspekte zum unternehmensübergreifenden Informationsaustausch eine Rolle spielen. So könnte beispielsweise die Aussage: „80 Prozent der Unternehmen aus der Handwerksbranche mit weniger als 200 Mitarbeitern investieren jährlich nicht mehr als 2000 Euro in ihre Virenschutzlösung“ einem Unternehmen wichtige Anhaltspunkte bei der Planung seiner Sicherheitsinvestitionen geben.

Aber nicht nur für Unternehmen kann ein überbetrieblicher Austausch im Themengebiet von Interesse sein. Auch für die Entwickler von Standards wie dem BSI verspricht eine überbetriebliche Datensammlung Vorteile, die in der aktiven Auswertung der Erfahrungen von Unternehmen bei der Umsetzung des Standards begründet liegen. Anhand der statistischen Untersuchung von Zeitstempeln kann während der Umsetzung des Realisierungsplanes analysiert werden, welche Maßnahmen typischerweise nacheinander realisiert werden. Beispielsweise muss der Maßnahme *M 2.25 Dokumentation der Systemkonfiguration* zwingend die Maßnahme *M 2.26 Ernennung eines Administrators und eines Vertreters* vorausgehen [Bun08b, S. 78]. Viele weitere Abhängigkeiten könnten durch den Einsatz einer kollaborativen Komponente ermittelt werden und deren Erkenntnisse in die Weiterentwicklung der Grundschutzkataloge und begleitenden Softwarewerkzeuge einfließen.

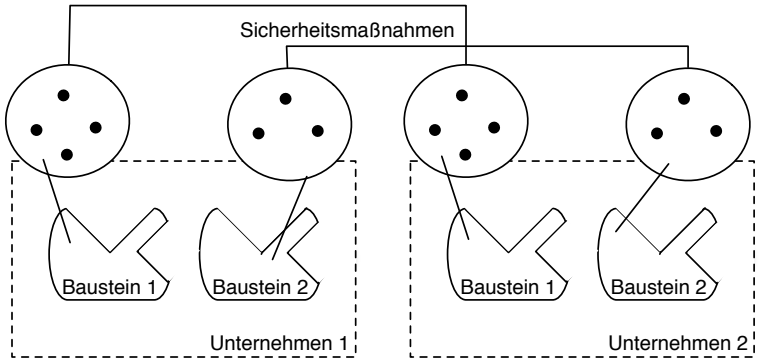

Abbildung 3: Zwei Unternehmen werden auf Basis der aktuellen Maßnahmenumsetzung in Bausteinen verglichen, die sie beide getrennt von einanander für ihr Unternehmen identifiziert haben.

Eine weitere Möglichkeit kollaboratives Sicherheitsmanagement zu betreiben, besteht darin, Unternehmen auf Basis von jeweils bereits durchgeführten BSI-Grundschutzanalysen miteinander zu vergleichen, um ab einer gewissen Ähnlichkeit den Unternehmen weitere passende Sicherheitsmaßnahmen zur Realisierung vorzuschlagen.

Innerhalb des Basis-Sicherheitschecks bewerten Unternehmen die Umsetzung von IT-Sicherheitsmaßnahmen für mehrere Bausteine (wie z. B. *allgemeiner Server* oder *Client unter Windows XP*) ihres Unternehmens. Die Antworten für die einzelnen in den Grundschutzkatalogen vorgeschlagenen Sicherheitsmaßnahmen, die jeweils einem Baustein zugeordnet sind, können dabei die folgenden Ausprägungen annehmen: Eine bestimmte IT-Sicherheitsmaßnahme wurde bisher *nicht umgesetzt*, *teilweise umgesetzt*, *umgesetzt* oder die Umsetzung ist *entberlich*. Zusätzlich dazu kann die jeweilige Einstufung mit einem Freitextfeld begründet und bereits eine erste Kostenabschätzung mit angegeben werden. In Abhängigkeit der Auswahl von Bausteinen und des aktuellen Umsetzungsgrades der entsprechenden Maßnahmen entsteht so für Unternehmen ein repräsentatives Muster. Vergleicht man auf dieser Ebene Unternehmen miteinander, lässt sich die Ähnlichkeit zweier Unternehmen zueinander ermitteln (vgl. Abbildung 3). Ähneln sich Unternehmen in einem Großteil ihrer gewählten Bausteine und deren Maßnahmenumsetzung, so könnten diese Unternehmen daran interessiert sein zu erfahren, welche weiteren Maßnahmen zur Absicherung von anderen Teilnehmern bereits umgesetzt wurden oder in Erwägung gezogen werden.

Dieses Verfahren könnte auch zur Plausibilitätskontrolle für die Eingabedaten von Unternehmen im Basis-Sicherheitscheck verwendet werden. Abbildung 4 verdeutlicht das anhand eines Vergleichs von neun Gruppen von Studenten, die im Rahmen einer Fallstudie [1] einen Basis-Sicherheitscheck für einen bestimmten Baustein durchgeführt haben. Da die Ausgangslage in diesem Beispiel für alle Gruppen die gleiche war, hätte man erwartet, dass alle Gruppen bei den paarweisen Vergleichen eine gewisse Ähnlichkeit aufweisen. Es

[1] Aufgabensammlung IT-Sicherheit: http://www-sec.uni-regensburg.de/intern/lecturenotes/AufgSec.pdf

Gleich eingestufte Maßnahmen normiert auf die gesamte Anzahl an Maßnahmen für den Baustein 'allgemeiner Client'

	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 5	Gr. 6	Gr. 7	Gr. 8	Gr. 9	alle A
Gr. 1		0,5	0,5	0,5	0,6	0,55	0	0,65	0,5	0
Gr. 2			0,55	0,5	0,55	0,45	0	0,55	0,5	0
Gr. 3				0,6	0,65	0,55	0,05	0,55	0,8	0,15
Gr. 4					0,75	0,65	0,05	0,65	0,5	0,05
Gr. 5						0,85	0	0,8	0,6	0
Gr. 6							0	0,8	0,5	0
Gr. 7								0	0,15	0
Gr. 8									0,5	0
Gr. 9										0,15

Abbildung 4: Ähnlichkeitsmatrix: Die Ähnlichkeit von neun unterschiedlichen Gruppen, die im Vorfeld ausgehend von einer Fallstudie einen Basis-Sicherheitscheck für den Baustein *B 3.201 allgemeiner Client* durchgeführt haben. Das Maß der Ähnlichkeit ist die Anzahl gleich eingestufter Maßnahmen im Bezug zu allen für diesen Baustein hinterlegten Maßnahmen (Vergleich der Istwerte). Diese Einstufung wird in der Spalte „alle A“ mit den in den Grundschutzkatalogen hinterlegten Sollwerten (Siegelstufe A) verglichen.

zeigte sich jedoch, dass in diesem Beispiel Gruppe 7 herausfällt, da sie im Rahmen der Fallstudie den besagten Baustein entweder vergessen oder im Zusammenhang für nicht relevant erachtet hat. In diesem Fall ist der direkte Vergleich leicht möglich, da alle Gruppen die gleiche Ausgangslage hatten. Auf die Praxis übertragen bedeutet dies, dass die Ähnlichkeit mehrerer Unternehmen erst durch den Vergleich der Maßnahmen aus Bausteinen ermittelt werden muss, um dann basierend auf diesen Ähnlichkeitsbeziehungen Eingabeüberprüfungen vornehmen zu können. Wenn z. B. mehrere Unternehmen bei einer Vielzahl von Bausteinen einen erhöhten Ähnlichkeitswert aufweisen und ein Unternehmen in einem Baustein Abweichungen wie in Abbildung 4 gezeigt aufweist, so kann eine Funktion zur Validitätskontrolle basierend auf Vergleichsdaten darauf hinweisen, dass an dieser Stelle bei dem Unternehmen noch Nacharbeitungsbedarf bestehen könnte.

Diese und weitere Untersuchungen werden erst durch eine zentrale Datensammlung ermöglicht.

3 Hauptanforderungen an ein System zum überbetrieblichen Datenaustausch

In [NF07, BESS11, HSF+09] und [Now11] werden bereits Anforderungen an Systeme zum überbetrieblichen Informationsaustausch beschrieben. Der Kontext liegt hierbei auf einer unternehmensübergreifenden Datensammlung zu Informationssicherheitsvorfällen, auf dem Austausch von Daten aus Security Information and Event Management Systemen (SIEM) sowie auf einem überbetrieblichen Vergleich in Echtzeit hinsichtlich sogenannter Key Performance Indikatoren (KPI). Die Anforderungen dieser artverwandten Arbeiten werden hier aufgegriffen und dienen als Ausgangslage für eine erste Anforderungserhebung zum kollaborativen IT-Sicherheitsmanagement.

Grundsätzlich lassen sich drei Hauptanforderungen an ein solches System ableiten, die in den folgenden Abschnitten kurz beschrieben werden:

- Das System muss für alle Teilnehmer Nutzen stiften.
- Das System muss den Schutz der Einzelunternehmen bestmöglich gewährleisten.
- Die Daten müssen sich ohne nennenswerten Mehraufwand erheben lassen.

3.1 Gebrauchstauglichkeit

Damit sich Unternehmen an einer übergreifenden Datensammlung beteiligen, muss der Nutzen, den eine solche Datensammlung im Sicherheitsmanagement mit sich bringt, herausgearbeitet und kommuniziert werden. Hierbei ist neben den Vorteilen für die Wissenschaft im Besonderen auch darauf zu achten, dass Unternehmen direkt aus den erhobenen Daten Vorteile erhalten, beispielsweise in Form einer ökonomischeren Maßnahmenauswahl oder einer effizienten Abfolge in der Realisierungsplanung.

Selbst innerhalb einer Branche können Unternehmen einen stark unterschiedlichen Aufbau ihrer IT-Landschaft aufweisen. Bei der Modellierung nach BSI-Grundschutz lassen sich eventuell nicht alle Eigenheiten adäquat abbilden. Auch die einzelnen Maßnahmen der Grundschutzkataloge weisen untereinander einen unterschiedlichen Detailierungsgrad auf. All diese Tatsachen erschweren eine einheitliche Vergleichbarkeit der Unternehmen. Eine notwendige Erfordernis für eine Plattform zum unternehmensübergreifenden Austausch von Informationen im IT-Sicherheitsmanagement ist es daher, Techniken und Metriken umzusetzen, die die genannten Nachteile bestmöglich ausgleichen und somit die Aussagekraft von Vergleichsdaten erhalten.

Weiter ist es erforderlich, dass Unternehmen kooperatives Verhalten beim Informationsaustausch an den Tag legen, da nur so die Gebrauchstauglichkeit des Informationssystems erhalten werden kann. Die beiden größten Probleme hierbei sind, dass Unternehmen motiviert sein könnten, lediglich Daten abzurufen ohne sich selbst an der Datensammlung zu beteiligen (vgl.[Now11, S. 187]) oder bewusst falsche Informationen zu übertragen. Das Übertragen falscher Informationen seinerseits kann entweder durch das Umgehen technischer Sperren motiviert sein, die Teilnehmern nur Daten zur Verfügung stellen, wenn diese auch zur Datensammlung beitragen, oder ggf. auch mit dem Ziel geschehen, möglichen Konkurrenten aktiv zu schaden (vgl. [Now11, S. 189], [BESS11]). Daher sind Lösungen anzustreben, die diesen negativen Auswirkungen bestmöglich entgegenwirken.

3.2 Teilnehmersicherheit

Ein weiterer Baustein im Spannungsfeld des kollaborativen IT-Sicherheitsmanagements sind Funktionen zum Schutz von Teilnehmerdaten und -identitäten. Daten zur geplanten Umsetzung von IT-Sicherheitsmaßnahmen beispielsweise geben genaue Auskunft über

ISBN 978-3-88579-286-4

den Ist-Zustand der jeweiligen Unternehmen bzgl. der IT-Sicherheit. Im Bekanntwerden und Zuordnen dieser Informationen zu Einzelunternehmen steckt erhebliches Bedrohungspotenzial. Aus diesem Grund müssen Techniken aus dem Bereich der Mehrseitigen Sicherheit [RPM96] gefunden und umgesetzt werden, die zum einen die Gebrauchstauglichkeit des Informationssystems erhalten und zum anderen allen teilnehmenden Unternehmen den bestmöglichen Schutz – sowohl vor anderen Teilnehmern, als auch vor dem Dienstbetreiber selbst – bieten.

Ein möglicher Lösungsansatz hierbei könnte sein, dass Unternehmen Daten zum Sicherheitsmanagement sammeln, noch in ihrem Schutzbereich von identifizierenden Merkmalen befreien (beispielsweise durch Überarbeiten oder Weglassen von identifizierenden Freitextinformationen im Basis-Sicherheitscheck), im Anschluss daran ihre Datensätze mit einem Geschäftsbeziehungspseudonym [SW07, S. 509] versehen und unter der Benutzung von Anonymisierungsdiensten wie JonDonym oder Tor[2] verschlüsselt an eine zentrale Stelle zur Auswertung schicken. Damit trotz der Verwendung von Pseudonymen in Verbindung mit dem anonymen Upload noch gewährleistet werden kann, dass es sich bei einer Übertragung um Daten von einem teilnehmenden Unternehmen handelt, wird beispielsweise in [Now11, S. 175f.] ein Verfahren vorgeschlagen, das blinde Signaturen im Zusammenhang mit der Pseudonymvergabe verwendet. Dabei handelt es sich um ein Verfahren, das auf [Cha82] basiert und das es einem Plattformbetreiber nach dem Upload von Datenpaketen ermöglicht, anhand einer Signatur festzustellen, ob es sich um Daten eines registrierten Teilnehmers handelt oder nicht, ohne jedoch das Pseudonym einem bestimmten Unternehmen selbst zuordnen zu können.

3.3 Unternehmensintegration

Die Erhebung von Daten zum Sicherheitsmanagement innerhalb von Unternehmen ist immer mit personellem Aufwand verbunden. Ist darüber hinaus zusätzlicher Aufwand notwendig, um die bereits einmal erhobenen Daten für einen unternehmensübergreifenden Datenaustausch erneut zu erheben, sinkt die Bereitschaft von Unternehmen, sich an einer gemeinschaftlichen Datensammlung zu beteiligen. Aus diesem Grund sollen nach Möglichkeit bestehende Informationssysteme bestmöglich genutzt werden, um kollaboratives IT-Sicherheitsmanagement zu ermöglichen. Laut [KWD+10, S. 49] sind die beiden meistbenutzten Werkzeuge im IT-Grundschutz derzeit das BSI-eigene *GSTOOL* und die Softwarelösung *verinice* (http://www.verinice.org). Mittels dieser Werkzeuge wird ein Großteil der in Tabelle 1 aufgezeigten Informationen bereits für die einzelnen Bausteine erhoben. Gelingt es, diese innerbetriebliche Informationssammlung für einen unternehmensübergreifenden Datenaustausch nutzbar zu machen (z. B. durch Erweiterung eines dieser Software-Werkzeuge oder Entwicklung einer Anwendung, die auf die gleiche Datenbasis zugreift), so lässt sich der Erhebungsaufwand gering halten. In eine solche Anwendung müssen auch die in Abschnitt 3.2 andiskutierten Schutzmaßnahmen integriert werden.

[2] Online erhältlich unter: http://www.jondonym.com/ und http://torproject.org/

4 Zusammenfassung

Mit dem vorliegenden Papier wurde eine Möglichkeit skizziert, die bisher vorhandenen Datenquellen zur Durchführung von BSI-Grundschutz um eine zusätzliche Datenquelle zur ökonomischen Entscheidungsfindung zu erweitern. Teilnehmende Unternehmen geben dabei Informationen zur Umsetzung von Sicherheitsmanagementmaßnahmen in Ihrem Unternehmen preis und können sich im Gegenzug mit anderen Unternehmen hinsichtlich Maßnahmenumsetzung und -kosten vergleichen. Wenn es gelingt, diese Daten unter Erhalt der Vergleichbarkeit sicher zwischen Unternehmen auszutauschen, können diese die Basis für zielgerichtete und angemessene Sicherheitsinvestitionen darstellen. Da die im eigenen Unternehmen erhobenen Daten zum Sicherheitsmanagement selbst einen erhöhten Schutzbedarf aufweisen, müssen Techniken zum Schutz der Vertraulichkeit der Identität genauso technisch umgesetzt werden, wie auch Techniken die eine innerbetriebliche Datenerhebung und eine aussagefähige Datenqualität garantieren. Auch eine Betrachtung der rechtlichen Aspekte wird im Zusammenhang einer überbetrieblichen Datensammlung, Speicherung und Verwendung notwendig. Dies werden die Aufgaben weiterer Forschungsarbeiten sein.

Dank

Die Autoren danken den Netzwerkpartnern des NIM-Projektes Regensburg, den anonymen Reviewern für hilfreiche Hinweise und Anmerkungen sowie der EU für die Förderung im Rahmen des EFRE-Projektes IT-Sicherheit.

Literatur

[BESS11] Henk Birkholz, Carsten Elfers, Bernd Samjeske und Karsten Sohr. Unternehmensübergreifender Austausch von sicherheitsrelevantem Wissen. *Datenschutz und Datensicherheit - DuD*, 35:258–261, 2011. 10.1007/s11623-011-0063-5.

[Bun08a] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS), 2008.

[Bun08b] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-2. IT-Grundschutz-Vorgehensweise, 2008.

[Bun08c] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz, 2008.

[Bun08d] Bundesamt für Sicherheit in der Informationstechnik. BSI-Standard 100-4. Notfallmanagement, 2008.

[Bun09a] Bundesamt für Sicherheit in der Informationstechnik. BSI IT-Grundschutz-Kataloge 11. Ergänzungslieferung - November 2009, 2009.

ISBN 978-3-88579-286-4

[Bun09b] Bundesamt für Sicherheit in der Informationstechnik. Pressemitteilung: Schutz vor Online-Vandalismus. IT-Grundschutz erhöht die Informationssicherheit, 2009.

[Cha82] David Chaum. Blind Signatures for Untraceable Payments. In *CRYPTO*, Seiten 199–203, 1982.

[Fed06] Hannes Federrath. Kosten und Nutzen der IT-Sicherheit. *Praxis der Wirtschaftsinformatik*, 248(2/2006):4–5, 2006.

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

[HSF+09] Dominik Herrmann, Florian Scheuer, Philipp Feustel, Thomas Nowey und Hannes Federrath. A Privacy-Preserving Platform for User-Centric Quantitative Benchmarking. In Simone Fischer-Hübner, Costas Lambrinoudakis und Günther Pernul, Hrsg., *Trust, privacy and security in digital business: 6th international conference, TrustBus 2009, Linz, Austria, September 3 - 4, 2009; proceedings*, Jgg. 5695 of *Lecture Notes in Computer Science*, Seiten 32–41. Springer, Berlin, Heidelberg, 2009.

[KWD+10] Stefan Kronschnabel, Stephan Weber, Christian Dirnberger, Elmar Török und Isabel Münch. IT-Sicherheitsstandards und IT-Compliance, 2010.

[NF07] Thomas Nowey und Hannes Federrath. Collection of Quantitative Data on Security Incidents. In *The Second International Conference on Availability, Reliability and Security (ARES 2007)*, 2007. erschienen in: The Second International Conference on Availability, Reliability and Security: ARES 2007; 10-13 April 2007, Vienna, Austria; proceedings. Los Alamitos, Calif.: IEEE Computer Society, 2007. ISBN 0-7695-2775-2, 978-0-7695-2775-8, S. 325-332.

[Now11] Thomas Nowey. *Konzeption eines Systems zur überbetrieblichen Sammlung und Nutzung von quantitativen Daten über Informationssicherheitsvorfälle*. Vieweg Teubner, Wiesbaden, 2011.

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

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

ISBN 978-3-88579-286-4