Expertenstudie zum Sicherheitsmanagement in deutschen Organisationen

Thomas Nowey, Hannes Federrath, Moritz Riesner
{thomas.nowey, hannes.federrath}@wiwi.uni-regensburg.de,
mriesner@gmail.com

Forschungsbericht
Universität Regensburg
Institut für Wirtschaftsinformatik
2009

Zusammenfassung

Vor dem Hintergrund wachsender Anforderungen wird das Sicherheitsmanagement in der Literatur zunehmend aus der Perspektive des Risikomanagements betrachtet. Für möglichst genaue Risikoanalysen ist eine quantitative Bewertung der Risikoparameter wünschenswert. Der vorliegende Forschungsbericht präsentiert die Ergebnisse einer deutschlandweiten Expertenstudie zum Stand des Informationssicherheitsmanagements in Unternehmen. Der erste Schwerpunkt der Studie sollte den Status Quo des Sicherheitsmanagements insbesondere im Hinblick auf die Verwendung von Risikomanagementansätzen und quantitativen Daten beleuchten. Gerade in kleinen und mittleren Unternehmen hat Informationssicherheitsmanagement nach Ansicht der Experten häufig noch einen zu geringen Stellenwert. Es wird häufig zu wenig systematisch vorgegangen und es mangelt an Unterstützung durch das Management. Die Autoren haben ein Konzept für eine Plattform zur überbetrieblichen Sammlung von Informationen über Sicherheitsvorfälle entwickelt, um damit eine Datenbasis für Risikobewertungen und Benchmarking aufzubauen, das im zweiten Teil der Studie evaluiert werden sollte. Die Experten empfanden den Ansatz als sehr positiv und sehen auch eine grundsätzliche Bereitschaft bei Unternehmen zum überorganisatorischen Datenaustausch. Allerdings formulierten sie auch zahlreiche Anforderungen an das System, von denen der Mehrwert für die Unternehmen und die Vertraulichkeit der Daten die wichtigsten sind.

1 Einführung

Eine zunehmende Zahl von Publikationen aus Wissenschaft und Praxis beschäftigt sich in den letzten Jahren mit dem Management von Informationssicherheit aus der Perspektive des operativen Risikomanagements (vgl. z.B. [BMG01]). Als Gründe für diese Entwicklung werden Faktoren wie zunehmende IT-Abhängigkeit der Geschäftsprozesse, Kostendruck, Compliance, die Notwendigkeit ökonomischer Begründbarkeit von Investitionsentscheidungen sowie die Integration in unternehmensweite interne Kontrollsysteme genannt. Die Ansätze zum Informationssicherheitsmanagement lassen sich in Best Practice Ansätze, qualitative Ansätze und quantitative Ansätze unterteilen [NFKP05]. Wie in anderen Wissenschaftsdisziplinen auch (vgl. [Woo61]) ist aus

theoretischer Sicht bei Risiken der Informationssicherheit eine Quantifizierung anzustreben. Das Ziel ist, Risiken in monetären Größen messbar zu machen. Die Publikationen im Bereich des quantitativen Risikomanagements konzentrieren sich ausgehend vom häufig kritisierten ROSI-Konzept meist auf das Entwickeln verbesserter Metriken und Methoden für die Risikosteuerung. Dabei wird die Existenz entsprechender quantitativer Daten zur Bewertung der Risiken oft vorausgesetzt. Verschiedene Autoren konstatieren jedoch, dass quantitative Daten kaum verfügbar sind (vgl. [Giu04], [BP07]).

Ausgehend von dieser in der Theorie bekundeten Datenlücke haben [NF07] ein Konzept für eine organisationsübergreifende Plattform zur Sammlung von relevanten Risikoparametern entwickelt. Dieses wird im folgenden Abschnitt kurz dargestellt. Das Konzept geht von der Annahme aus, dass in der einzelnen Organisation nicht ausreichende Datenmengen für eine umfassende Risikoidentifikation und Bewertung vorliegen und dass sich Informationen über Vorfälle in der Vergangenheit grundsätzlich zur Prognose der künftigen Risikosituation eignen, wie z.B. auch vom Basler Ausschuss für Bankenaufsicht vertreten wird ([Bas03]).

Die vorliegende Expertenstudie hatte nun einerseits das Ziel zu überprüfen, ob der in der Theorie vorhandene Bedarf an quantitativen Daten in der Praxis auch tatsächlich nachweisbar ist und welche Informationen Praktiker für ein verbessertes Risikomanagement benötigen. Andererseits sollte das Konzept der Austauschplattform auf seine Praxistauglichkeit überprüft werden. Zudem sollte das Wissen der Experten dazu beitragen, neue Ansätze, Ideen und Forschungsfragen in diesem Bereich zu identifizieren.

Das Papier ist wie folgt gegliedert. Abschnitt 2 gibt einen kurzen Überblick über ähnliche Untersuchungen. In Abschnitt 3 wird das Grundkonzept einer Austauschplattform für Vorfallsinformationen vorgestellt. Abschnitt 4 beschreibt darauf aufbauend die Zielsetzung der Expertenstudie. Nach der Erläuterung der Forschungsmethodik in Abschnitt 5 präsentiert Abschnitt 6 die wichtigsten Resultate der Studie und die Implikationen für das Forschungsprojekt. Abschließend gibt Abschnitt 8 einen Ausblick auf weitere Forschungsfragen und Herausforderungen.

2 Stand der Forschung

Verschiedene Untersuchungen versuchen regelmäßig ein Bild der Informationssicherheit in Organisationen zu zeichnen. Besonders prominente Vertreter sind die von <kes> und Microsoft durchgeführte Sicherheitsstudie [kes08] oder der CSI/FBI Report [Ric07], die beide im jährlichen Rhythmus herausgegeben werden. Daneben sind zahlreiche Studien insbesondere von Beratungsunternehmen verfügbar. Die beiden erstgenannten nutzen eine große Grundgesamtheit und eine relativ breite Zielgruppe, die Befragung erfolgt jedoch bei nahezu allen Studien mit Hilfe stark standardisierter Fragebögen, die entweder versandt oder im Interview ausgefüllt werden. Durch ausführliche Fragebögen wie bei der <kes>/Microsoft-Sicherheitsstudie können detaillierte Aussagen zum Status Quo der IT-Sicherheit getroffen werden. Aus dieser starken Standardisierung folgt auch eine starke Orientierung an „harten Fakten“. Der Status Quo wird zwar umfassend erhoben, jedoch lassen sich über die Hintergründe nur schwer aussagen treffen. Dies gilt insbesondere für die Frage, wie Entscheidungen für Sicherheitsmaßnahmen getroffen werden und welche Bedeutung quantitative Risikomanagementansätze für den Bereich der Informationssicherheit haben. Genau mit diesen Aspekten sollte sich die vorliegende Untersuchung beschäftigen.

Den Autoren ist lediglich eine einzige Untersuchung bekannt, die sich konkret mit

der Sammlung von Informationen zu Sicherheitsvorfällen beschäftigt. Die ENISA hat im Auftrag der EU europaweit 60 Institutionen identifiziert, welche sich mit der Sammlung von Informationen über Sicherheitsvorfälle beschäftigen [Cas07]. Als mögliche Datenquellen wurden Umfrageergebnisse ebenso identifiziert wie CERTs oder Informationen von Herstellern von Sicherheitssoftware. Ziel war die Gewinnung genereller Erkenntnisse über ein Framework zur Datensammlung und wie diese Innitativen möglicherweise kombiniert werden könnten. In einem abschließenden Fragebogen und einem Workshop mit 17 Teilnehmern wurden auch Möglichkeiten und Voraussetzungen zum Informationsaustausch in diesem Bereich diskutiert. Allerdings lag dieser Betrachtung kein konkretes Konzept über den Austausch zu Grunde.

Der zweite Teil der vorliegenden Untersuchung baut auf den Erkenntnissen und Forderungen der ENISA-Untersuchung auf, da diese einige erste Hinweise auf mögliche Forderungen und Einschränkungen gibt, welche bei der Konzeption des Leitfadens berücksichtigt wurden. Allerdings wurde im vorliegenden Fall ein konkretes Szenario für den Informtionsaustausch geschildert und als Zielgruppe wurden Experten gewählt, die tatsächlich mittelbar oder unmittelbar für mögliche Datenlieferanten tätig sind.

3 Forschungsprojekt

Grundidee des in [NF07] präsentierten Konzepts ist es, eine technische Plattform zu schaffen, um quantitative Daten zu IT-Sicherheitsvorfällen zu sammeln, aufzubereiten und bereitzustellen und so die verfügbare Datengrundlage für das Management der Informationssicherheit der teilnehmenden Organisationen zu verbessern sowie theoretische Erkenntnisse über Informationssicherheitsrisiken zu gewinnen. Als Vorbild dienen Schadensdatenbanken wie sie in Banken und Versicherungen zu anderen Zwecken (Kreditausfälle, Versicherungsfälle) bereits seit langer Zeit erfolgreich eingesetzt werden (vgl. [Rö02]) und wie sie beispielsweise vom Basler Ausschuss für das Management operativer Risiken empfohlen werden (vgl. [Bas03]). Auch auf EU-Ebene wird der Austausch von Informationen über Sicherheitsvorfälle als vielversprechend angesehen [Cas07].

Abbildung 1 zeigt eine schematische Darstellung der Austauschplattform. Kern des Konzepts ist eine Vielzahl von teilnehmenden Organisationen, welche Informationen über Sicherheitsvorfälle in ihrer Organisation erfassen und an eine zentrale Stelle übermitteln. Diese sammelt und systematisiert die Daten, führt Aggregationen durch und stellt die aufbereiteten Informationen anschließend den Teilnehmern wieder zur Verfügung. Der so erzeugte Datenbestand soll um Daten aus externen Quellen angereichert werden. Im Gegensatz zu existierenden Konzepten, die sich häufig die Früherkennung von neuen Angriffen zum Ziel gesetzt haben, soll der Schwerpunkt bei den zu erhebenden Daten auf den **Auswirkungen der Vorfälle** liegen. Die gewonnenen Daten sollen die Teilnehmer beim Informationssicherheitsmanagement unterstützen.

Durch die organisationsübergreifende Datensammlung wird insbesondere eine größere Datenbasis geschaffen. Dies ist nach Ansicht der Autoren insbesondere im Hinblick auf sogenannte LFHI-Risiken (Low Frequency High Impact) besonders wichtig. Würde man nur die Vorfälle der einzelnen Organisation betrachten, wäre die Gefahr groß, einzelne Risiken zu über- oder unterschätzen oder schlimmstenfalls gar nicht zu berücksichtigen. Zusätzlich werden auch organisationsübergreifende Vergleiche ermöglicht. Durch die Konzentration auf die Auswirkungen der Vorfälle sollen echt quantitative Daten zu möglichen Schadenshöhen ermöglicht werden. Statt qualitativer Bewertungen könnten Risiken so systematisch abgeschätzt und in Geldeinheiten

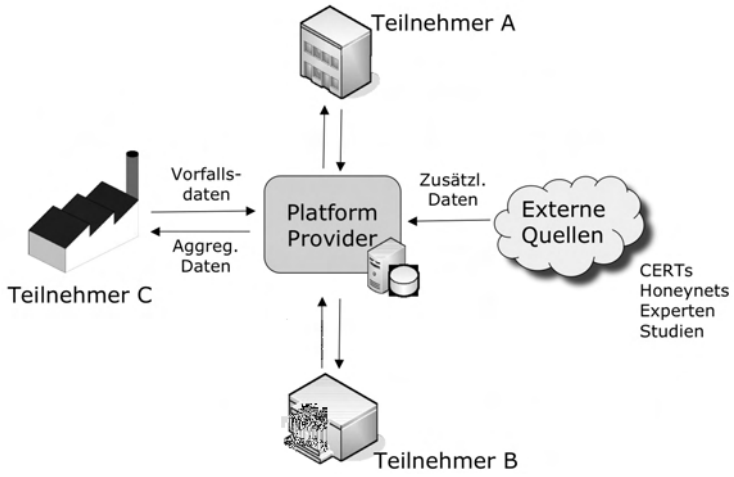

Abbildung 1: Plattform

bewertet werden.

Auf theoretischer Ebene wurden bereits Anforderungen an die Plattform identifiziert. Hierzu zählen Sicherheit (insbesondere Vertraulichkeitsanforderungen), Fairness, eine einheitliche Sprache zur Beschreibung der Vorfälle sowie Usability-Aspekte. Eine konkrete Implementierung scheint jedoch ohne Berücksichtigung der tatsächlichen Anforderungen der Praxis wenig sinnvoll.

4 Zielsetzung

Die Zielsetzung der Studie war zweigeteilt. Ein Ziel bestand darin, Informationen über das momentan betriebene Sicherheitsmanagement in Organisationen zu sammeln, um hieraus zu ermitteln, ob ein Bedarf an quantitativen Daten besteht, den die Austauschplattform bedienen könnte. Dazu war es wichtig, herauszufinden, auf welcher Basis Entscheidungen im Sicherheitsmanagement getroffen werden und welche Rolle quantitative Daten dabei spielen. Dabei war auch die Verfügbarkeit dieser Daten im Unternehmen von Interesse sowie die Frage, ob unternehmensinterne Daten für Entscheidungen ausreichen.

Es sollten auch Informationen über die Schwerpunkte und den Organisationsgrad des momentan in der Praxis betriebenen Sicherheitsmanagements gesammelt werden, um diese möglicherweise in die Ausgestaltung der Austauschsplattform einfließen zu lassen.

Ein weiteres Ziel war es, das Konzept der vorgestellten Austauschplattform evaluieren zu lassen. Hier ging es zunächst um die Bewertung der Idee als solche und um die Akzeptanz in der Wirtschaft sowie um Kritierien, die vor einem Praxiseinsatz erfüllt sein müssen. Von Interesse war in diesem Zusammenhang auch, ob bereits ähnliche Konzepte existieren. In einem nächsten Schritt wollten wir weitere Anhaltspunkte zur Gestaltung der Plattform sammeln. Im Vordergrund standen die Anforderungen an die entstandenen Daten und deren bevorzugte Einsatzmöglichkeiten sowie potentielle Betreiber und die Art der Beteiligung von Unternehmen.

5 Methodik

Als Zielgruppe für das Experteninterview wählten wir vom BSI zertifizierte Auditoren. Durch den Einsatz in verschiedenen Unternehmen, IT-Beratungen und öffentlichen Einrichtungen, sowohl als Auditor wie auch als Berater, haben sie einen weit reichenden Überblick über das IT-Sicherheitsmanagement in der Praxis. Aus den Rückmeldungen ergaben sich mit 23 der angeschriebenen Auditoren auswertbare Interviews.

Zwischen qualitativer und quantitativer Forschung besteht ein Spannungsverhältnis. Eine verbalisierte, also qualitative, Befragung bietet den Vorteil, dass sie inhaltlich reichhaltigere Resultate ermöglicht und die Befragten ihre Meinung näher erläutern können. Eine quantitative Befragung lässt sich hingegen leichter durchführen und ermöglicht einfachere Vergleiche. Viele Forschungsprojekte kombinieren inzwischen beide Herangehensweisen [BD06].

Für eine systematisierende Expertenbefragung, die zur systematischen und lückenlosen Informationsgewinnung dient, eignet sich nach Bogner und Menz ein relativ ausdifferenzierter Leitfaden, der auch durch standardisierte Fragen ergänzt werden kann [BM05]. Das von uns gewählte leidfadengestützte Interview eignet sich, da das Thema durch die Komplexität und die verschiedenen Hintergründe der Befragten allein numerisch mit standardisierten Fragen nur schwer abgedeckt werden kann.

Der Leitfaden gibt dem Befrager eine Gespächsstruktur vor und verhindert, dass das Gespräch zu weit zu irrelevanten Themen abschweift [MN05]. Gleichzeitig erlaubt er, vorher nicht antizipierte Fragestellungen anzubringen, lässt also Abweichungen zu [BD06]. Dadurch bleibt der Gesprächsverlauf variabel, die Antworten zu den einzelnen Fragen bleiben aber dennoch vergleichbar.

Mit geschlossenen Fragen zum Ende der Gespräche sollte die Meinung des Experten in Zahlen gefasst werden, um statistische Auswertungen zu ermöglichen. Der Fragebogen wurde durch ein Probeinterview auf Verständlichkeit und angemessene Dauer getestet und verbessert. Die angestrebte Dauer der Gespräche war 30-45 Minuten.

Dem inhaltlichen Teil des Leitfadens ging eine kurze Erhebung zum beruflichen Hintergrund des befragten Auditors voran. Inhaltlich waren die Gespräche in drei Teile unterteilt: Zunächst ging es um die aktuelle Situation des Sicherheitsmanagements und danach um die Bewertung der Austauschplattform. Zuletzt wurden die geschlossenen Fragen gestellt. Diese bestanden aus Aussagen, zu denen der Befragte seine Zustimmung auf einer fünfstufigen Skala ausdrücken konnte.

Mit den Auditoren, die sich zu einem Interview bereit erklärt hatten, haben wir telefonisch Termine vereinbart. Die Gespräche wurden entweder aufgezeichnet und später transkribiert oder direkt protokolliert.

Bei der Auswertung orientierten wir uns an den möglichen Arbeitsschritten einer qualitativen Auswertung, die Bortz grob beschreibt [BD06]. Unsere Auswertung des qualitativen Teils erfolgte nach den einzelnen Fragen des Leitfadens, die nach den ersten beiden Teilbereichen gegliedert waren. Durch diese Einteilung war das entstandene Material bereits grob vorstrukturiert. Dennoch war es nötig, Antworten, die über die jeweilige Fragestellung hinausgingen, ggf. anderen Fragen zuzuordnen. Die Zusammenstellung der Antworten für jede einzelne Fragestellung ermöglichte es, je Frage einen zusammenfassenden Eindruck des Meinungsbildes zu gewinnen. Zur Verarbeitung der Antworten verwendeten wir eine Tabellenkalkulation und wiesen jedem geführten Interview eine Zeile und jeder Fragestellung eine Spalte zu.

Bortz [BD06] beschreibt die Möglichkeit, quantitative in qualitative Daten zu transformieren, beispielsweise durch die Auszählung von Schlüsselbegriffen. Dies erwies sich bei einigen Fragestellungen als nützlich, beispielsweise bei der Frage nach aktuel-

len Trends im Sicherheitsmanagement. Es ermöglichte auch, Einzelmeinungen von oft geäußerten Meinungen abzugrenzen.

6 Ergebnisse der Interviews

Alle befragten Auditoren konnten auf umfangreiche Erfahrungen im Bereich der Informationssicherheit verweisen. Ihre tatsächlichen Positionen, Tätigkeitsprofile und Aufgabenfelder sind indes sehr heterogen. Dies ermöglichte eine sehr vielschichtige Betrachtung der Themenfelder. Der überwiegende Teil der Studienteilnehmer ist für Beratungs- und Prüfungsunternehmen im Bereich der Informationssicherheit tätig. Dabei werden in der Regel sowohl Beratungs- als auch Auditierungsprojekte betreut. Die übrigen Teilnehmer kommen aus Wissenschaft und Forschung oder sind in Organisationen für die interne Informationssicherheit tätig. Die Teilnehmer konnten über Erfahrungen mit Unternehmen unterschiedlichster Größen (von KMU bis hin zu Konzernen) und Branchen berichten. Neben einer Vielzahl an Erfahrungen mit privatwirtschaftlichen Unternehmen, flossen auch einige Berichte aus Organisationen der öffentlichen Hand in die Ergebnisse ein.

Die Darstellung der Ergebnisse der Studie erfolgt in zwei Schwerpunkten: Zunächst werden die Resultate zum Status Quo des Sicherheitsmanagments in Organisationen vorgestellt, anschließend folgt die Auswertung zum interorganisatorischen Datenaustausch. Die zum Abschluss eines jeden Interviews gestellten geschlossenen Fragen wurden den zwei Schwerpunkten zugeordnet.

6.1 Informationssicherheitsmanagement allgemein

Zunächst wurden die Experten nach ihrer allgemeinen Einschätzung zu **Status und Trends des Sicherheitsmanagements** in Organisationen befragt. Bei den Experten herrscht relative Einigkeit, dass es nicht mehr genügt, rein technische Aspekte wie Virenschutz oder Firewalls zu betrachten, sondern dass systematisches Sicherheitsmanagement mit Beachtung von Prozessen und organisatorischen Aspekten an Bedeutung gewonnen hat. Compliance wird als wichtiger Treiber für Sicherheitsmanagement gesehen. Damit verbindet sich auch die Hoffnung, dass externe Auflagen zu einer stärkeren Systematisierung des Sicherheitsmanagements und zur Sensibiliserung der Entscheidungsebene in Organisationen führen. Allgemein wird ein mangelndes Bewusstsein für die Bedeutung der Informationssicherheit bei den Entscheidern beklagt. Dies liegt offenbar auch daran, dass Informationssicherheit in der Organisationshierarchie oft auf einer unteren Ebene angesiedelt ist.

Ein sehr heterogenes Bild ergibt sich bezüglich der **Systematik des Vorgehens**. Mit der Ausnahme von stark IT-abhängigen Organisationen wie Rechenzentren wurde das Sicherheitsmanagement in kleineren und mittleren Unternehmen überwiegend als unsystematisch bezeichnet. Bei größeren Organisationen sind hingegen häufig entsprechende Prozesse und Strukturen etabliert, wobei auch hier noch Verbesserungsbedarf gesehen wird. Eine starke Korrelation sehen die Befragten bezüglich Systematisierungsgrad und Zertifizierung. Viele Organisationen führen im Zuge einer Zertifizierung überhaupt erst ein systematisches Informationssicherheitsmanagement ein. Dies erklärt möglicherweise auch, warum viele der Befragten sowohl beratend als auch auditierend tätig sind. Die Unternehmenslandschaft lässt sich also unterteilen in Firmen, die bereits aktives Sicherheitsmanagement betreiben, zumeist nach einem Standard (ISO 27001, Grundschutz) und in Firmen, bei denen dies noch nicht etabliert ist.

Die befragten Experten halten es für wünschenswert, dass **Investitionsentscheidungen** im Bereich der Informationssicherheit auf Basis eines geplanten Vorgehens zum Risikomanagement getroffen werden. In der betrieblichen Praxis sind ihrer Einschätzung nach jedoch die häufigsten Auslöser für Sicherheitsmaßnahmen vorangegangene Sicherheitsvorfälle. Weiterhin wird IT-Sicherheit oft nur als Kostenfaktor gesehen und ausreichende Mittel erst nach eingetretenen Vorfällen bereitgestellt. Es wird also eher reagiert als antizipiert. Treiber für ein geplantes Vorgehen sind auch hier drohende Strafen durch die Verletzung von Gesetzen oder Auflagen und die Erfüllung von Standards. Wird ein geplantes Vorgehen angewandt, so orientieren sich Organisationen meist an Best Practices, zunehmend eingebunden in einen Risikomanagementkreislauf. Auf ökonomischen Prinzipien basierende Methoden aus Investitionstheorie oder Entscheidungslehre sind nur in Einzelfällen anzutreffen.

Diejenigen Organisationen, die bereits ein systematisches Informationssicherheitsmanagement etabliert haben, bemühen sich auch, **Risiken zu bewerten**. Die relevanten Parameter, Eintrittswahrscheinlichkeit und Schadenshöhe, werden meist qualitativ bestimmt (z.B. niedrig, mittel, hoch). Nur vier der Befragten Experten gaben an, dass das Management von Informationssicherheitsrisiken in den ihnen bekannten Organisationen zumindest zum Teil mit Hilfe quantitativer Daten erfolgt. Hingegen sagten 17 Experten aus, dass dies wünschenswert wäre (vgl. 2). Die Vorteile werden dabei insbesondere in der größeren Objektivität und der besseren Integration in das Risikocontrolling des Gesamtunternehmens gesehen. Die Abschätzung von Eintrittswahrscheinlichkeiten und Schadenshöhen auf Basis von subjektiven Urteilen birgt das Risiko einer Über- oder Unterschätzung bestimmter Risiken. Unternehmen, die quantitative Daten nutzen, greifen überwiegend auf unternehmensintere Daten zurück. Mehr als die Hälfte der Experten ist jedoch überzeugt, dass die vorhandenen internen Daten nicht ausreichend für das Risikomanagement sind und sogar mehr als zwei Drittel sehen in fehlenden Daten eine wesentliche Hürde für quantitatives Risikomangement. Als wesentliche Quellen für externe Daten wurden insbesondere externe Berater, CERT-Dienste, Studien, Newsletter und Umfrageergebnisse genannt.

Sicherheitsvorfälle, die sich in der eigenen Organisation ereignet haben, werden in fast allen Unternehmen, die ein Informationssicherheitsmanagementsystem etabliert haben erfasst und dokumentiert. Meist bildet diese Dokumentation die Grundlage für spätere Sicherheitsmaßnahmen. Hinsichtlich des Detaillierungsgrades gibt es jedoch erhebliche Unterschiede. Nach Auskunft der Experten existieren hierzu keine einheitlichen Prozesse oder Werkzeuge. Nur größere Organisationen verfügen über Softwarelösungen, die eine Vorfallserfassung unterstützen. Als Hauptziel der Vorfallserfassung wurde die Verhinderung eines wiederholten Eintritts des gleichen Vorfalls genannt.

Die Ergebnisse des Teilbereichs lassen sich wie folgt zusammenfassen. Dort wo bereits ein Sicherheitsmanagement nach einem etablierten Standard eingeführt wurde, ist dies meist auch systematisch. Größere Firmen sind oft organisierter als kleinere. Hier gibt es einen geregelten Entscheidungsprozess (z.B. Plan-Do-Check-Act-Kreislauf) zu IT-Sicherheitsmaßnahmen. In diesem Falle kommt es auch zur systematischen Erfassung, Sammlung und Verwendung von quantitativen Daten im Sicherheitsmanagement, beispielsweise zur Risikoquantifizierung. In Konzernen bzw. Konzerngruppen kommt es intern auch zum Austausch von Daten zum Sicherheitsmanagement. Über die firmeninternen Daten zu Sicherheitsvorfällen hinaus halten die meisten Befragten externe Daten für nützlich, stellen jedoch die Verwendbarkeit von unternehmensfremden Daten in Frage. Genutzte Quellen für zusätzliche Daten sind CERT-Dienste, externe Berater oder Veröffentlichungen von Instituten wie dem BSI. In vielen Firmen, be-

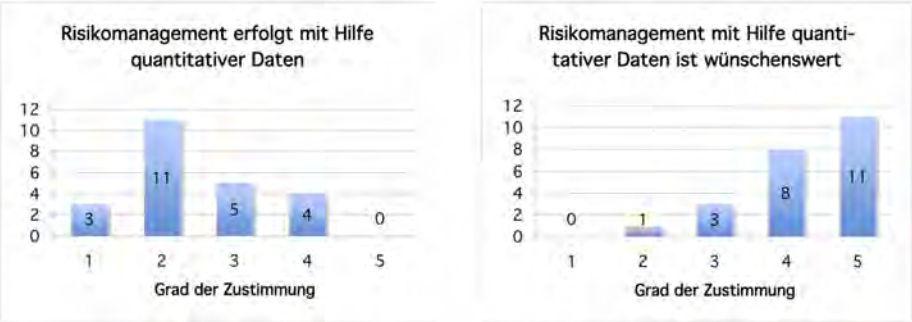

Abbildung 2: Quantitative Daten im Management von Informationssicherheitsrisiken

sonders kleinen und mittelständischen Unternehmen wird noch keine Notwendigkeit für organisiertes Sicherheitsmanagement gesehen. Entscheidungen zu Sicherheitsmaßnahmen werden hier meist anlassbezogen getroffen, also nach eingetretenen Schäden oder durch externen Druck, z.B. durch regulatorische Massnahmen oder Wünsche des Kunden.

6.2 Überbetrieblicher Datenaustausch

Wie oben dargestellt, ist der überwiegende Teil der Experten der Ansicht, dass Informationssicherheitsrisiken auf Basis von quantitativen Daten bewertet und gesteuert werden sollten. Gleichzeitig werden die innerhalb der Organisationen verfügbaren Daten als nicht ausreichend gesehen. Genau diese Lücke versucht die in Abschnitt 3 beschriebene Austauschplattform zu schließen. Den Studienteilnehmern ist noch kein vergleichbares Projekt bekannt. Zwar wurden einige Initativen zum Austausch von Informationen und Wissen über das Sicherheitsmanagement genannt, jedoch handelt es sich dabei meist um einen informellen Austausch beispielsweise innerhalb von Arbeitskreisen. In Sicherheitslösungen wie Firewalls und Intrusion Detection Systeme integrierte Berichtsfunktionen melden zwar Daten an den Hersteller, erfassen aber nur einen kleinen Ausschnitt der großen Bandbreite von Vorfällen und betrachten nicht den entstandenen Schaden. Weiterhin wurde der Austausch von Informationen über operative Risiken innerhalb von Konzernverbünden genannt. Insbesondere der Einbezug der Auswirkungen des Vorfalls wurde als innovativ bezeichnet.

Die Idee der Austauschplattform für quantitative Daten zu Sicherheitsvorfällen wurde von den meisten Befragten positiv gesehen, lediglich 3 von 23 Teilnehmern hielten das Konzept für nicht sinnvoll oder nicht durchführbar. 17 der befragten Experten sind der Ansicht, dass der Informationsaustausch den Unternehmen einen Mehrwert liefern würde. Verbunden mit dieser positiven Grundeinstellung war aber auch Skepsis bezüglich der konkreten Einführung im Unternehmen. Dies zeigt sich nicht zuletzt an den Antworten auf die Frage nach der Bereitschaft von Unternehmen, am Datenaustausch teilzunehmen (vgl. Abb. 3). Die Bereitschaft zur Teilnahme war in unserer Untersuchung jedoch bereits deutlich höher als in eingangs zitierter ENISA-Studie. Dies liegt vermutlich daran, dass das System im vorliegenden Fall bereits detaillierter beschrieben werden konnte.

Die Verwendung von historischen Daten sehen die Experten trotz verschiedener Einschränkungen als den einzigen probaten Weg zur Bestimmung der Größen für eine Risikoabschätzung. Sie plädierten jedoch zugleich für die Kombination dieser Daten

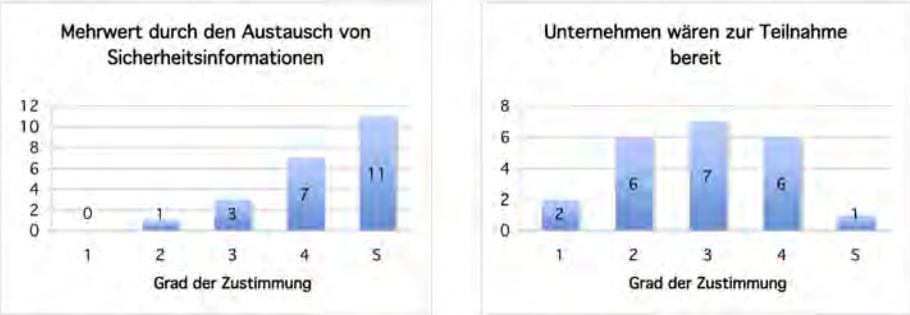

Abbildung 3: Einschätzung zum Konzept der Plattform

mit Experten- und Erfahrungswissen. Hinsichtlich der Verfügbarkeit von Informationen über Sicherheitsvorfälle zeigten sich die Befragten optimistisch. Zwar würden die meisten Informationen heute noch nicht systematisch erfasst, prinzipiell seien die Daten jedoch vorhanden.

Die größte Schwierigkeit sehen die Studienteilnehmer darin, Unternehmen zur Teilnahme zu bewegen. Dies kann nur gelingen, wenn einige Hauptanforderungen erfüllt werden. Die zwei Hauptforderungen waren:

- **Wahrung der Vertraulichkeit**. Die wesentliche Hürde für die Teilnahme von Organisationen an der Plattform sehen die Experten in der Sensibilität der zu übermittelnden Daten. Unternehmen werden ihrer Ansicht nach nur dann ihre Daten zur Verfügung stellen, wenn die Daten ausreichend anonymisiert sind. Die größte Gefahr wird darin gesehen, dass Informationen über Sicherheitsvorfälle an die Öffentlichkeit gelangen könnten. Bezüglich der Ausgestaltung dieser Anomyisierung herrschte Konsens darüber, dass unbedingt sichergestellt werden muss, dass Externe nicht erfahren können, welcher Vorfall sich in welchem Unternehmen ereignet hat. Auch innerhalb des geschlossenen Teilnehmerkreises muss diese Vertraulichkeit gewährleistet werden. Idealzustand nach Meinung einiger Befragter wäre Pseudonymität auch dem Betreiber der Plattform gegenüber, wobei das Vertrauen in den Plattformbetreiber als entscheidender Faktor genannt wurde.

- **Aufzeigen eines Mehrwerts**. Weitere Bedingung ist ein klarer, erkennbarer Nutzen für Unternehmen, die dafür ja sensible Daten weitergeben sowie Mitarbeiterzeit aufwenden müssen. Da prinzipiell kein anderer Weg gesehen wird, an vergleichbare Daten zu kommen, ist ein solcher Nutzen auch nach Meinung der Befragten durchaus gegeben. Darüber hinaus muss die Erfassung von Vorfällen einfach und mit überschaubarem Aufwand möglich sein. Die Experten bemängelten neben der Datenqualität der heute verfügbaren Informationen vor allem den großen Aufwand bei der Datenbeschaffung. Es wurde als äußerst mühsam bezeichnet, aus der großen Menge an verfügbaren Reports und Studien die relevanten Informationen zu extrahieren. Eine zentrale Infromationsquelle mit hochwertigen Daten wird daher als echter Vorteil gesehen.

Insbesondere die Forderung nach Anonymisierung und Schutz vertraulicher Informationen zeigt, dass bei der Konzeption des Austausches ein Trade-Off nötig ist. Es muss abgewägt werden zwischen Datenqualität und Anonymisierungsgrad. Besonders

Abbildung 4: Vorfallserfassung in Organisationen

die Übertragbarkeit der Ergebnisse von einer Organisation auf die andere hängt maßgeblich von Parametern wie Branche oder Unternehmensgröße ab, die aber auch bessere Rückschlüsse auf die Organisation zulassen, in der sich der Vorfall ereignet hat. Hier gilt es eine geeignete Balance zu finden.

Einen wesentlichen Mehrwert sehen die Experten in der Möglichkeit zum Benchmarking. Denkbar sind Auswertungen, um zu erfahren, wie viele Sicherheitsvorfälle im eigenen Unternehmen im Vergleich mit ähnlichen Unternehmen der Branche auftreten und ob sich die Schadenshöhe unterscheidet.

Bezüglich der Beschaffenheit der zu erhebenden Informationen, war aus Expertensicht die Vergleichbarkeit der Datensätze das wichtigste Kriterium.

Hinsichtlich der Frage, wer eine solche Plattform betreiben sollte, ergab sich kein einheitliches Bild. Als wichtigstes Kriterium für die Auswahl wurde die Vertrauenswürdigkeit hinsichtlich der Geheimhaltung der Daten aufgeführt. Außerdem sollte der Betreiber ohne Eigeninteresse sein. Einigkeit herrschte hinsichtlich der Feststellung, dass dies nach Möglichkeit keine Institution sein sollte, die mit den Daten selbst kommerzielle Zwecke verfolgt oder verfolgen könnte, wie beispielsweise ein Anbieter von Sicherheitslösungen. Als mögliche Betreiber wurden staatliche Stellen wie das BSI ebenso genannt wie Universitäten, Genossenschaften oder etablierte privatwirtschaftliche Institutionen, die bereits über entsprechendes Vertrauen verfügen. Jeder genannte Kandidat hat jedoch bei anderen Befragten Bedenken hervorgerufen. Neben der Vertrauenswürdigkeit des Betreibers an sich sollte ein entsprechendes Vertragswerk und nach Meinung einiger Befragter auch Zertifizierungen die bestimmungsgemäße Verwendung der Daten sicherstellen.

Neben den bereits vom Interviewer genannten Verwendungsmöglichkeiten der Daten für das Sicherheitsmanagement (insbesondere Benchmarking und Schätzung von Risikoparametern) könnten sich die Teilnehmer auch vorstellen, die Daten zu nutzen um

- Führungskräfte zu überzeugen,
- Awareness im Unternehmen zu erzeugen,
- die Kosten/Effizienz des Sicherheitsmanagements zu bewerten,
- bestehende Standards, Vorgehensweisen und Ratgeber zum IT-Sicherheitsmanagement zu evaluieren und zu verbessern.

7 Implikationen für die Plattform

Zusammenfassend ergeben sich folgende Implikationen für die Entwicklung der Plattform.

Die wichtigste Anforderung an die vorgestellte Austauschplattform ist, dass die Vertraulichkeit der Daten sichergestellt ist. Um das Vertrauen der möglichen Teilnehmer zu gewinnen, sollte sie transparent gestaltet werden und keine den Interessen der Teilnehmer entgegenstehenden Zwecke verfolgen. Die Rückführbarkeit von Daten auf Teilnehmende Unternehmen muss wirksam verhindert werden, beispielsweise durch Aggregation von Datensätzen. Ideal wäre Pseudonymität für die teilnehmenden Unternehmen auch gegenüber den Betreibern. Ungeachtet der technischen Realisierung ist die Schaffung einer Vertrauensbasis erforderlich. Sowohl zwischen den Teilnehmern als auch zwischen Teilnehmern und Plattformbetreiber muss ein Vertrauensverhältnis bestehen. Eine geschlossene Nutzergruppe mit genau definierten Aufnahmekriterien und einem vertraglichen Rahmenwerk erscheint als sinnvolle Möglichkeit.

Der Nutzen muss für die Unternehmen klar erkennbar sein: Soweit es die zugesicherte Vertraulichkeit erlaubt, sollten die bereitgestellten Daten möglichst detailliert sein, um die Vergleichbarkeit und Verwendbarkeit im eigenen Unternehmen zu ermöglichen. Auch weitere Einsatzmöglichkeiten für das Unternehmen sollten bei der Gestaltung berücksichtigt werden. Hier ist insbesondere der Benchmarking-Aspekt hervorzuheben, der von vielen Teilnehmern als noch wichtiger als die Ableitung von Risikoparametern empfunden wurde. Eine weitere interessante Anregung für den Ausbau der Plattform ist die Spezialisierung auf spezielle Szenarien oder Anwendungen. Dies erschien den Experten vor allem für komplexe Lösungen sinnvoll, die in vielen Unternehmen in unterschiedlichen Ausprägungen eingesetzt werden. Als Beispiel seien hier SAP-Anwendungen genannt.

8 Fazit und Ausblick

Die gewählte Methode des leitfadengestützten Experteninterviews hat sich bewährt. Sie wurde auch von den Interviewten als sehr positiv empfunden, da sie die Möglichkeit zu differenzierteren Aussagen und Begründungen liefert.

Aus Expertensicht besteht ein Trend zur Einführung von aktivem und bewusstem IT-Sicherheitsmanagement, insbesondere eingebunden in das Risikomanagement des gesamten Unternehmens. Wo dieses betrieben wird, kommt es auch zu systematischer Erfassung und Bewertung von Sicherheitsvorfällen und es gibt einen geregelten Entscheidungskreislauf. Dort, wo Sicherheitsmanagement nicht oder nicht organisiert betrieben wird, werden Sicherheitsvorfälle nicht systematisch erfasst und Entscheidungen erst nach eingetretenen Vorfällen oder aufgrund von subjektiven Einschätzungen oder spontanen Ideen getroffen. Die Befragung hat ergeben, dass unternehmensinterne Daten für das an Bedeutung gewinnende Sicherheitsmanagement nicht ausreichen und der Austausch von Daten einen Mehrwert bieten würde.

Größere Firmen tendieren eher zu systematischem Sicherheitsmanagement als kleine und mittelständische Firmen, wo noch viel Nachholbedarf besteht. Oft liegt dies am mangelndem Bewusstsein des Managements. Sicherheitsmanagement wird hier als Kostenfaktor der IT und nicht als Managementaufgabe gesehen.

Externe quantitative Daten zu Sicherheitsvorfällen werden für das Sicherheitsmanagement benötigt. Diese müssen jedoch auf die eigene Situation anwendbar sein, was von den Befragten als Herausforderung gesehen wird. Der überbetriebliche Datenaus-

tausch wird im Allgemeinen positiv bewertet. Die vorgestellte Plattform könnte aus Sicht der Experten eine Lösung sein, wenn die Anforderungen hinsichtlich Vertraulichkeit und Mehrwertgenerierung erfüllt werden. Dann kann auch mit einer entsprechenden Beteiligung gerechnet werden, wobei trotzdem Aufklärungs- und Überzeugungsarbeit nötig sein wird.

Der nächste Schritt bei der Entwicklung des Systems ist die Fertigstellung des Prototypen unter Berücksichtigung der Resultate der Studie. Insbesondere die Möglichkeiten zum Schutz der Anonymität der Daten und die Auswertung zu Benchmarkingzwecken sollen verbessert werden. Hierzu ist insbesondere zu evaluieren, in wie weit datenschutzfreundliche Techniken anwendbar sind und für welche Auswertungen sich Mehrparteienberechnungsprotokolle zur Wahrung der Anonymität einsetzen lassen. Anschließend werden die Teilnehmer der Studie und weitere interessierte Unternehmen zu einem Testbetrieb eingeladen und gebeten, das System und insbesondere die zu Grunde liegende Taxonomie zu evaluieren.

9 Danksagung

Die Durchführung dieser Studie wurde durch die Unterstützung durch zahlreiche Personen und Organisationen ermöglicht. Die Autoren bedanken sich inbesondere bei allen befragten Experten, Isabell Münch, Bundesamt für Sicherheit in der Informationstechnik und unseren Kollegen am Lehrstuhl Management der Informationssicherheit.

Literatur

[Bas03] Basel Committee on Banking Supervision. Sound practices for the management and supervision of operational risk, February 2003.

[BD06] Jürgen Bortz and Nicola Döring. *Forschungsmethoden und Evaluation*, chapter Qualitative Auswertungsmethoden, pages 296–350. Springer, 2006.

[BM05] Alexander Bogner and Wolfgang Menz. *Das Experteninterview*, chapter Das theoriegenerierende Experteninterview., pages 33–70. Verlag für Sozialwissenschaften, 2 edition, 2005.

[BMG01] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 97–104, New York, NY, USA, 2001. ACM Press.

[BP07] Walter S. Baer and Andrew Parkinson. Cyberinsurance in it security management. *IEEE Security & Privacy*, 5(3):50–56, May/June 2007 2007.

[Cas07] Carsten Casper. Examining the feasibility of a data collection framework. Technical report, European Network and Information Security Agency, November 2007.

[Giu04] Paolo Giudici. *Operational Risk Modeling and Analysis*, chapter Integration of Qualitative and Quantitative Operational Risk Data: A Bayesian Approach, pages 131–138. Risk Books, 2004.

[kes08] kes. Fragebogen für die <kes>/microsoft-sicherheitsstudie 2008. *<kes>*, 24(1):67–82, März 2008.

[MN05] Michael Meuser and Ulrike Nagel. *Das Experteninterview*, chapter ExpertInnenintervies - vielfach erprobt, wenig bedacht, pages 71–93. VS Verlag für Sozialwissenschaften, 2 edition, 2005.

[NF07] Thomas Nowey and Hannes Federrath. Collection of quantitative data on security incidents. In *Proceedings. The Second International Conference on Availability, Reliability and Security.*, pages 325–332, 2007.

[NFKP05] Thomas Nowey, Hannes Federrath, Christian Klein, and Klaus Plößl. Ansätze zur evaluierung von sicherheitsinvestitionen. In Hannes Federrath, editor, *Sicherheit 2005. Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit*, number P-62 in Lecture Notes in Informatics, pages 15–26. Köllen-Verlag, 2005.

[Ric07] Robert Richardson. Csi computer crime and security survey 2007, 2007.

[Rö02] Sven A. Röckle. *Schadensdatenbanken als Instrument zur Quantifizierung von Operational Risk in Kreditinstituten*. Verlag Wissenschaft & Praxis, 2002.

[Woo61] Harry Woolf, editor. *Quantification. A History of the Meaning of Measurement in the Natural and Social Sciences*. The Bobbs-Merrill Company, Inc., 1961.