3-4-2015

QUANTSEC - Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen

Golriz Chehrazi

Christopher Schmitz

Oliver Hinz

QUANTSEC – Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen

Golriz Chehrazi[1], Christopher Schmitz[2] und Oliver Hinz[3]

[1] Technische Universität Darmstadt, Deutschland
golriz.chehrazi@ec-spride.de
[2] Goethe-Universität Frankfurt, Deutschland
christopher.schmitz@m-chair.de
[3] Technische Universität Darmstadt, Deutschland
hinz@emarkets.tu-darmstadt.de

Abstract. IT-Sicherheitsmaßnahmen unterstützen den sicheren Software-Entwicklungsprozess und tragen zur Reduktion von Angriffen und Schwachstellen bei. Art und Ausmaß einzusetzender Sicherheitsmaßnahmen beruhen in der Regel auf ökonomischen Kosten-Nutzen-Abwägungen. In dieser Arbeit wird ein generisches kennzahlenbasiertes Modell zur ökonomischen Wirkungsanalyse implementierter Sicherheitsmaßnahmen vorgestellt. Dazu werden technische und ökonomische Wirkungszusammenhänge und zugehörige, objektiv messbare Kennzahlen, wie z.B. Erkennungs- und Korrekturzeiten sowie Ursachenklassen, erarbeitet. Das Wissen um Wirkungszusammenhänge ermöglicht Analysen zur Messung des Nutzens implementierter Sicherheitsmaßnahmen. Der Einsatz des Modells wird exemplarisch anhand von Maßnahmen der Bedrohungsanalyse illustriert. Mit Hilfe statistischer Methoden können die Auswirkungen von Sicherheitsmaßnahmen und deren Nutzen quantifiziert werden. Das Modell, der Nutzen und die praktische Anwendbarkeit werden in sechs Experteninterviews diskutiert.

Keywords: IT-Sicherheitsmaßnahme, Bewertung, Ökonomischer Nutzen, Quantifizierung, Statistische Analyse

1 Motivation

Die Durchführung von IT-Sicherheitsmaßnahmen ist ein kostspieliger Prozess, dessen Nutzen schwer direkt messbar ist [1]. Eine objektive Nutzenbewertung der Maßnahmen trägt dazu bei, ihre Wirkungsweise besser zu verstehen, ihren Einsatz ökonomisch, d.h. auf Basis von Kosten-Nutzen-Bewertungen, zu rechtfertigen und IT-Sicherheitsprozesse zu optimieren. So können z.B. sicherheitsrelevante Aspekte im Entwicklungsprozess aufgedeckt, Defizite der Sicherheitsmaßnahmen und besonders aufwändig zu behebende Software (SW)-Attribute wie Schwachstellentypen identifiziert und belegt werden.

12th International Conference on Wirtschaftsinformatik,
March 4-6 2015, Osnabrück, Germany

Chehrazi, G.; Schmitz, C.; Hinz, O. (2015): QUANTSEC - Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen, in: Thomas. O.; Teuteberg, F. (Hrsg.): Proceedings der 12. Internationalen Tagung Wirtschaftsinformatik (WI 2015), Osnabrück, S. 1131-1145

IT-sicherheitsrelevante Informationen werden in IT-Unternehmen bereits in verschiedenen Prozessen verarbeitet, z.B. bei der Analyse und Korrektur von Schwachstellen und Angriffen. Damit sind die Voraussetzungen für automatisierte Datenerfassungs- und statistische Analyseprozesse gegeben, die Rückschlüsse auf den Nutzen von Maßnahmen erlauben. In dieser Arbeit wird ein hierarchisches Modell zur objektiven, kontinuierlichen und zu einem Großteil automatisierbaren Messung des Nutzens von IT-Sicherheitsmaßnahmen vorgestellt. Dieses setzt sich zusammen aus den Kosten der Maßnahmen und den dadurch erzielten Kostenersparnissen. Dazu werden technische und ökonomische Wirkungsbeziehungen von Modellen unterschiedlicher Abstraktionsgrade erarbeitet und um objektiv messbare Kennzahlen zur automatisierten Datenerfassung ergänzt. Mit Hilfe statistischer Methoden können auf Grundlage der erfassten Datenbasis unternehmensindividuelle Gewichtungen sicherheitsrelevanter Gegebenheiten berechnet und ökonomische Verbesserungen der IT-Sicherheitsprozesse initiiert werden. Das Besondere hierbei ist die objektive, automatisierbare Berechnung im Gegensatz zu der herkömmlichen Vorgehensweise über subjektive Expertenschätzungen. Durch die kontinuierliche Datensammlung können zudem Veränderungen im Zeitverlauf erkannt und analysiert werden.

Die Anwendung des Modells wird anhand von Maßnahmen der Bedrohungsanalyse einer Software-as-a-Service (SaaS) Anwendung illustriert. Die wichtigsten Wirkungsbeziehungen des Modells, die Verfügbarkeit der erforderlichen Daten und der Aufwand für die Datensammlung werden in sechs Experteninterviews diskutiert.

2 Ansätze zur Messung des Nutzens von Sicherheitsmaßnahmen

Existierende Ansätze zur Wirtschaftlichkeitsbewertung von IT-Sicherheitsmaßnahmen behandeln zumeist ex-ante-Bewertungen zu tätigender Investitionen. Soo Hoo unterscheidet Modelle der ersten und zweiten Generation [3]. Die Modelle der ersten Generation sind Low-Level-Ansätze, die präzise, quantitative Daten zu Eintrittswahrscheinlichkeiten und Auswirkungen von Schadensereignissen als Berechnungsgrundlage voraussetzen. Häufig basieren sie auf der Annual Loss Expectancy (ALE), der (jährlichen) Verlusterwartung durch IT-Sicherheitsangriffe. Da hierzu i.d.R. keine exakten Daten vorliegen, sind Schätzungen erforderlich, wodurch die Resultate sehr verzerrt werden können [2-3]. Die „Valuation-Driven Methodologies“, als Vertreter der zweiten Generation, sind stärker operationalisierte Middle-Level-Konzepte, die dem Informationsdefizit der ALE-basierten Methoden durch vereinfachende Methoden wie der internen Verrechnung mit Risikomatrizen begegnen. Da die Eingabewerte häufig subjektiven Beurteilungen unterliegen, wird die Realität mitunter stark verzerrt abgebildet [3]. Factor Analysis of Information Risk (FAIR), ein Rahmenwerk, das Faktoren zur Bestimmung des Informationsrisikos eines Assets in Beziehung zueinander setzt, zählt zu diesen Methodologien. Dessen Taxonomie beschreibt grundlegende ökonomische und technische Wirkungsbeziehungen, die sich auf den Schaden auswirken können, und strukturiert diese systematisch [4]. Darüber hinaus existieren einzelne, abstrakte High-Level-Konzepte wie der

breiter gefasste Return-on-Security-Investment (ROSI)-Ansatz [5] ohne Angaben zur konkreten Berechnung.

Die vorgestellten Methoden werden kritisiert wegen der Abhängigkeit der errechneten Werte von Schätzungen [5], wegen in der Praxis nicht verfügbarer Daten und wegen fehlender Vorgabe einheitlicher, operativ messbarer Kennzahlen zur Erfassung von Schaden und Ersparnissen. Die Schwierigkeit der Erfassung objektiver Daten für die Berechnungen ist somit ein Hauptgrund des Verzichts auf analytische Bewertungsverfahren [6]. Dieses Defizit zeigt sich ebenso bei existierenden Ansätzen zur ex-post-Evaluation von IT-Sicherheitsmaßnahmen [7] wie auch in ebenenübergreifenden Ansätzen. In [8] werden objektiv messbare Kennzahlen mit subjektiven Expertenschätzungen zur Bewertung von Bedrohungen kombiniert. Andere Ansätze zur Maßnahmenbewertung verwenden hauptsächlich subjektive, empirisch erhobene Daten (vgl. [9]) und sind somit schwer generalisierbar, wiederholbar oder validierbar.

Um die beschriebenen Modelldefizite zu beheben, wurde QUANTSEC (**Quant**ifying **Sec**urity) entwickelt, ein ebenenübergreifendes Modell zur Nutzenbewertung von Sicherheitsmaßnahmen, das auf Basis objektiv und operativ messbarer Unternehmenskennzahlen arbeitet.

3 QUANTSEC – Ein Modell zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen

Die Verknüpfung messbarer, objektiver Sicherheitskennzahlen (vgl. [10]) mit ökonomischen Ansätzen erlaubt eine automatisierte Messung sicherheitsrelevanter unternehmenspezifischer Gegebenheiten und Zusammenhänge, und einer darauf aufbauenden Bewertung des Sicherheitsniveaus von Systemen und Anwendungen. Die systematische Sammlung zugehöriger Kennzahlen ermöglicht objektive, d.h. konsistente, vergleichbare und wiederholbare Messungen. Statistische Analysen zeigen die Wirkungsstärken der Kennzahlen zueinander auf und werden zudem dazu verwendet, die Effektstärke durchgeführter Maßnahmen auf die im Modell definierten Kennzahlen zu bestimmen. Dies ermöglicht unterschiedliche Analysen zur Bewertung ökonomischer Auswirkungen implementierter Sicherheitsmaßnahmen, wie z.B. über deren Nutzen, so dass der Prozess laufend verbessert werden kann. Zudem liefern die historischen Daten fundierte Schätzwerte für Prognosen. Das Modell wird anhand der Bedrohungsanalyse eines SaaS-Anwendungsszenarios zur Nutzenbewertung illustriert, um das Vorgehen zur Ermittlung messbarer Kennzahlen beispielhaft vorzustellen. Dieses kann auf andere Sicherheitsmaßnahmen übertragen werden.

Der Ansatz von Soo Hoo [3] dient als Grundlage für QUANTSEC. Die drei Kernkomponenten des Modells sind: *Sicherheitskosten C (Costs), Ersparnisse S (Savings)* und *Schadenshöhe L (Loss)*. Der ökonomische Nutzen von IT-Sicherheitsmaßnahmen resultiert vor allem aus Angriffsreduktionen und daraus entstehenden Schadensreduktionen sowie Ersparnissen durch die frühzeitige Schwachstellenerkennung und -behebung. Dem Vergleich zur Nutzenbestimmung der Maßnahmen wird jeweils ein fixer Zeitabschnitt, z.B. 6 Monate, zugrunde gelegt. Die Ausgangssituation dient als Baseline und wird der Ist-Situation nach Durchführung der Maßnahmen gegenüberge-

stellt. Ist der Wert positiv, so ergibt sich ein finanzieller Nutzen. Dies veranschaulicht folgende Formel:

$$\text{Nutzen} = (L_{Baseline} - L_{Ist}) - C + S_{Ist} \quad (1)$$

mit
$L_{Baseline}$, L_{Ist} = Schaden (Loss) vor bzw. nach Maßnahmendurchführung
C = Kosten (Costs) der Maßnahmen
S_{Ist} = Ersparnisse (Savings) durch Maßnahmen

Die **Schadenskomponente L** (Losses) gibt das finanzielle Ausmaß von Angriffen wider. Sie berechnet sich aus der Angriffshäufigkeit und der Schadenshöhe. Die **Kostenkomponente C** (Costs) beschreibt die Kosten, die für die Durchführung der Sicherheitsmaßnahmen anfallen. Als Ausgangsbasis für die Kostenstruktur dient der bilanzorientierte Total-Cost-of-Ownership (TCO)-Ansatz [11]. Wir verwenden ein einperiodisches Modell, da wir eine rückblickende Perspektive auf getätigte Maßnahmen einnehmen, zugehörige Kosten für Hardware, SW und Outsourcing i.d.R. einmaliger Natur sind und auch kontinuierlich anfallende Kosten dadurch abgebildet werden können. Auf die Kostenkomponente wird in dieser Arbeit nicht eingegangen, weil darin finanzielle Kennzahlen im Vordergrund stehen, deren Messung offensichtlich ist. Des Weiteren integriert QUANTSEC in Anl. an [12] **Ersparnisse**, die durch eine frühe Schwachstellen-Identifikation und -Korrektur von Schwachstellen realisiert werden können. Dieses Verfahren wird in unserer Arbeit stärker operationalisiert und durch die Integration der Post-Release-Phase als zusätzliche Entstehungsphase für Schwachstellen erweitert.

Bevor wir die Komponenten detaillierter beschreiben, werden die für die statistischen Analysen notwendigen Attribute in Abb. 1 visualisiert. Je nach Verfügbarkeit sind diese einer Schwachstelle oder einem Angriff zuzuordnen. Angriffe werden dabei über ausgenutzte Schwachstellen beschrieben.

Abb. 1. Analyseattribute von Schwachstellen und Angriffen

Ein Großteil dieser Informationen wird in vielen Unternehmen bereits erhoben, insbesondere bei großen SW-Entwicklungsfirmen. Diese adressiert unser Modell in erster Linie. Dabei ist nicht die vollständige Sammlung ausschlaggebend, sondern die systematische Sammlung als Basis für statistische Auswertungen. Je Angriff ist das attackierte Schutzziel, der zugehörige Bedrohungstyp, wie z.B. Denial-of-Service, und Entdeckungs- und Behebungszeitpunkt zu protokollieren. Des Weiteren ist der Datensatz um Attribute der ausgenutzten Schwachstelle zu ergänzen, die lokalisationsbasiert bei der Angriffsanalyse aufgedeckt werden. Dazu zählt der Schwachstellentyp, z.B. laut Common Weakness Enumeration (CWE), die Lokalisation der SW-

Komponente, der Schweregrad nach CVSS (Common Vulnerability Scoring System) sowie der unternehmensindividuelle Schweregrad. Letztere spiegelt das finanzielle Schadensausmaß der Schwachstellen-Ausnutzung wider. Abgeleitet werden kann er z.B. auf Basis einer Kombination von ermittelter Priorität des Schwachstellenscanners, rechtlichen und regulatorischen Anforderungen und der Kritikalität betroffener Assets bzw. Anwendungen sowie betroffener Kunden. SW-Entwicklungsfirmen verwenden i.d.R. ein intern festgelegtes System zur Priorisierung von Schwachstellen. Die systematische Speicherung dieser Informationen, auch wenn nicht vollständig vorhanden, ermöglicht statistische Auswertungen, deren Ergebnisse zur Bewertung von Schwachstellenanalysen in Abhängigkeit ihrer ökonomischen Relevanz und zur Nutzenbewertung durchgeführter Maßnahmen eingesetzt werden können. Hilfreiche Indikatoren zur Ursachenforschung einer Schwachstelle sind die Herkunft einer Komponente, z.B. ob sie extern entwickelt wurde oder ob es sich um eine Open Source (OSS) Komponente handelt oder auch, ob die Schwachstelle intern oder extern entdeckt wurde. Da Schwachstellen-Anzahl mit Größe und Komplexität der Anwendungen korreliert, sind die Codezeilen (Lines of Code – LoC) nützlich zur Normalisierung der Werte. Die Tabelle kann durch zusätzliche Attribute für weiterführende Analysen ergänzt werden. Die Verknüpfung der Modellkomponenten, die Wirkungsbeziehungen und die zu erhebenden Kennzahlen, die exemplarisch im weiteren Verlauf erläutert werden, sind in Abb. 2 dargestellt.

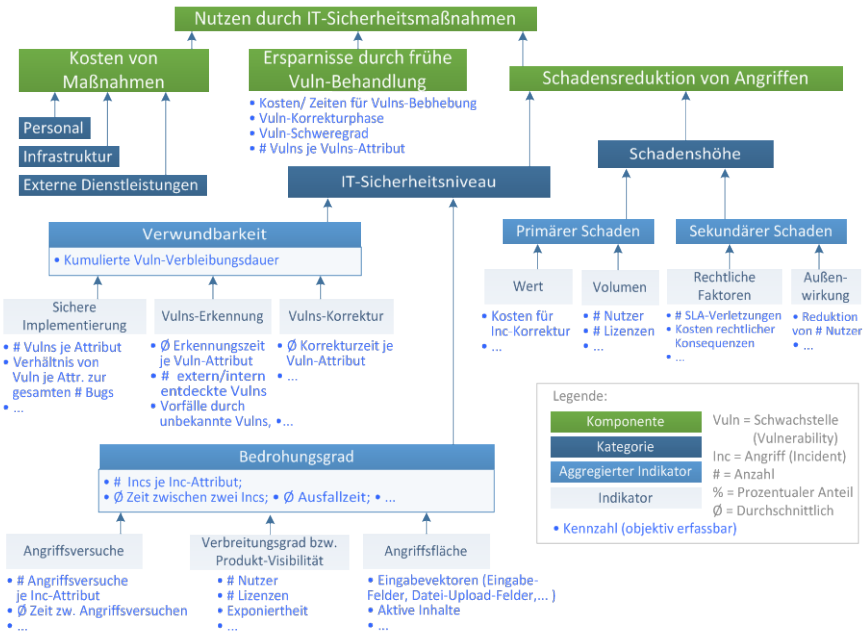

Abb. 2. Modellüberblick

Die Ausgestaltung der **Schadenskomponente** basiert auf den angepassten und um Kennzahlen erweiterten Wirkungsbeziehungen der FAIR-Taxonomie [4]. Neben der

Berechnung der Schadenshöhe werden die Beziehungen zwischen den Indikatoren für die statistischen Analysen verwendet, indem Wirkungsstärken zwischen diesen errechnet werden. Das **IT-Sicherheitsniveau** wird bestimmt durch die *Verwundbarkeit* und den *Bedrohungsgrad* einer Anwendung.

Der **Bedrohungsgrad** beschreibt den Ausnutzungsgrad von Schwachstellen. Als approximierte Metrik für dessen Messung kann die Ausfallzeit von Anwendungen durch Angriffe verwendet werden, ebenso wie die Angriffshäufigkeit, die für Analysen zusätzlich nach verschiedenen Attributen kategorisiert werden kann. Der Bedrohungsgrad wird in folgende drei Indikatoren unterteilt:

1. Die **Angriffsfläche** repräsentiert die Menge aller denkbaren Angriffswege, um Zugang zu einem System zu erlangen. Kennzahlenklassen zur Messung der Angriffsfläche werden in [13] beschrieben. Dazu zählen Eintrittspunkte (EP), d.h. Methoden über die Daten in das System gelangen, z.B. unsichere Formularfelder oder Authentifizierungsmethoden, Austrittspunkte (AP), nicht vertrauenswürdige Daten (NVD) und Kommunikationskanäle (KK).
2. **Produkt-Visibilität und Verbreitungsgrad**: Eine hohe Produkt-Sichtbarkeit und eine große öffentliche Wahrnehmung erhöhen die Anzahl potenzieller Angreifer und somit auch den Bedrohungsgrad. Kennzahlen zur Messung des Verbreitungsgrads sind z.B. die Anzahl verkaufter Lizenzen oder die Exponiertheit, d.h. die öffentliche Zugänglichkeit.
3. **Angriffe und Angriffsversuche:** In der Literatur wird die Angreiferperspektive [4] als zusätzliche Determinante des Bedrohungsgrads einer Anwendung verwendet. Da diese schwierig objektiv zu erfassen ist, verwenden wir stattdessen die Anzahl der Angriffe und Angriffsversuche.

Zusätzlich wird das IT-Sicherheitsniveau durch die **Verwundbarkeit** bestimmt. Diese spiegelt die Stärke und Effektivität des sicheren Software-Entwicklungsprozesses im Allgemeinen und der Sicherheitsmaßnahmen im Speziellen wider. Sie kann durch die kumulierte Schwachstellen-Verweilzeit (Korrektur- minus Entstehungsphase) gemessen werden. Die folgenden drei Indikatoren werden in Anlehnung an [10] zur Bewertung verwendet:

1. **Sichere Implementierung:** Zur Messung der sicheren Implementierung, die das Sicherheitsniveau der Design- und Entwicklungsaktivitäten widerspiegelt, dient die Anzahl aller bekannten Schwachstellen.
2. **Erkennung***:* In das System eingeführte Schwachstellen müssen zur Korrektur erkannt werden. Die Wirksamkeit dieses Indikators kann durch die durchschnittliche Erkennungszeit gemessen werden, d.h. der Zeitraum zwischen der Einführung einer Schwachstelle und dessen Erkennung oder durch die Anzahl von Vorfällen, die unbekannte Schwachstellen ausgenutzt haben.
3. **Korrektur**: Die Korrektur lässt sich durch die durchschnittliche Zeit zwischen Erkennung und Korrektur einer Schwachstelle messen.

Zum Normieren der Häufigkeitsdaten können die Kennzahlen zur Messung des Bedrohungsgrads herangezogen werden, z.B. die Angriffshäufigkeit mit der Anzahl verkaufter Lizenzen oder der Kundenanzahl, da eine steigende Nutzerzahl positiv mit der Anzahl entdeckter Schwachstellen korreliert.

Die **Schadenshöhe** berechnet sich auf Grundlage der Angriffe. Es wird unterschieden zwischen dem *primären Schaden* und dem *externen Schaden***.** Der **primäre Schaden** adressiert den direkten Schaden und subsumiert die Indikatoren *Wert* und *Volumen*. **Wert** beschreibt den Angriffsschaden, der sich vor allem aus den Kosten der Angriffsbehandlung berechnet, z.B. den Korrektur- und Auslieferungskosten. Das **Volumen** beschreibt Einflussfaktoren der Schadenshöhe wie die Anzahl betroffener Kunden und generierter Umsätze je Kunde. **Sekundärer Schaden** stellt Kosten dar, die sich nicht direkt auf die Anwendung beziehen. Sie werden unterteilt in rechtlicher Schaden und Schaden durch negative Außenwirkung als Konsequenz erfolgreicher Angriffe wie z.B. Reputationsschäden.

Die **Erparniskomponente** $\mathbf{S}_{IST}$ (**S**avings), berechnet die Ersparnisse durch frühe Schwachstellenbehebung, indem die Kosten für die Korrektur von Schwachstellen aufgeschlüsselt und für eine fixe Periode vor und nach Durchführung der Maßnahmen miteinander verrechnet werden. In Abhängigkeit der Entstehungs- und der Korrekturphase von Schwachstellen werden die attributspezifischen Korrekturkostensätze ($KorrK_{i,j}$) auf Basis einer exemplarischen Schwachstellenmenge ermittelt[1]. Optional können zusätzliche Attribute in der Auswertung berücksichtigt werden, wie z.B. der Schweregrad, der unterschiedliche Korrekturaufwände in Abhängigkeit von Schwachstellentyp und -brisanz in der Post-Release-Phase reflektiert. Dann wird die attributspezifische Anzahl gefundener Schwachstellen ($Vuln_{i,j \text{ bzw. } k}$) auf Basis der Anwendungsgröße und der Anzahl an Schwachstellen je Attribut-Kombination normalisiert und den Kostensätzen zugeordnet. Die Ersparnisse ergeben sich aus der Differenz nach Anwendung der Maßnahmen. Die Berechnung lässt sich wie folgt formalisieren:

$$S_{Ist} = \sum_{i=1,j=1}^{i=m,j=n} \#Vuln_{i,j} * KorrK_{i,j} * \left(\frac{\#Vuln_{i,j}(t_{Baseline})}{\sum_{k=1}^{n} \#Vuln_k(t_{Baseline})} - \frac{\#Vuln_{i,j}(t_{Ist})}{\sum_{k=1}^{n} \#Vuln_k(t_{Ist})}\right) \quad (2)$$

mit

$\#Vuln_{i,j \text{ bzw. } k}$ = Anz. der Schwachstellen mit Entsehungsphase i und Korrekturphase j bzw. k

$KorrK_{i,j}$ = Schwachstellen-Korrekturkosten mit Entstehungsphase i und Korrekturphase j

$t_{Baseline}$, t_{Ist} = Zeitintervall vor bzw. nach Maßnahmendurchführung

m, n = Menge aller Entstehung- bzw. Korrekturphasen

In Abb. 3 wird beispielhaft eine Berechnung anhand von drei Attribut-Kombinationen für die gefundenen Schwachstellen durchgeführt, woraus sich Ersparnisse in Höhe von 33.750 € ergeben[2]. QUANTSEC ermöglicht die quantitative Nutzenberechnung von Sicherheitsmaßnahmen, wenn die zugrundeliegenden Kennzahlen vorliegen. Da uns noch keine Anwendungsdaten in auswertbarer Form zur Verfügung stehen, demonstrieren wir im nächsten Kapitel nur die Machbarkeit der statistischen Berechnungen anhand eines fiktiven Beispiels.

[1] Verfahren zur Approximation der Kostensätze sowie Beschreibungen zur Errechnung von Ersparnissen durch frühzeitiges Beheben von SW-Fehlern sind in [12] zu finden.

[2] Zur vereinfachenden Darstellung ist in Abb. 3 die Anzahl der Schwachstellen vor und nach Durchführung der Maßnahmen gleich.

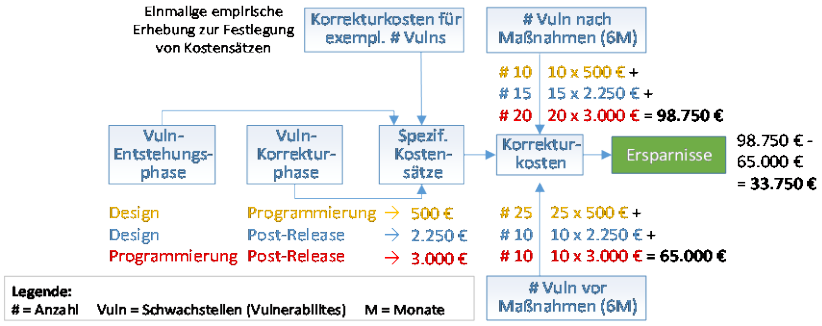

Abb. 3. Ersparnisberechnungsmodell durch frühes Beheben von Schwachstellen

4 Modellanwendung anhand von Maßnahmen eines Software-as-a-Service Anwendungsszenarios

4.1 Vorgehen zur Anwendung von QUANTSEC

Folgend wird beispielhaft das Vorgehen zu QUANTSECs Anwendung anhand eines SaaS-Szenarios illustriert. Hierbei wird angenommen, dass das SW-Unternehmen die Anwendung selbst hostet. Eine exakte, separierte Nutzenmessung einzelner Maßnahmen ist durch vorhandene Wechselwirkungen zwischen diesen oftmals nicht sinnvoll. Daher wird in Abschnitt 4.3 skizziert, wie QUANTSEC zur Nutzenbewertung des Maßnahmenbündels, bestehend aus einer Bedrohungsanalyse und der daraus resultierenden Sicherheitsmaßnahmen, angewendet werden kann.

4.2 Nutzenberechnung der Sicherheitsmaßnahmen

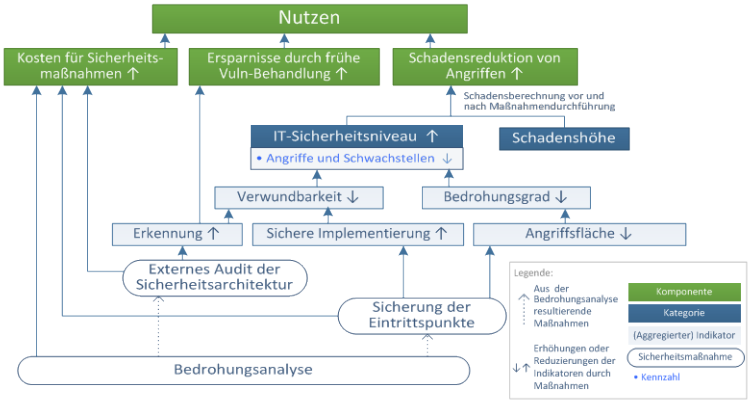

Abb. 4. Wirkungsanalyse der Sicherheitsmaßnahmen

Für jede Maßnahme (Maßn) sind zunächst die Wirkungsbeziehungen zu und Auswirkungen auf die Modellkomponenten zu spezifizieren. Die Zuordnung dieser objektiv messbaren Kennzahlen erlaubt eine indikatorenübergreifende Analyse der erhobenen Daten als Ausgangsbasis für Verbesserungen der Maßnahmen. Abb. 4 visualisiert diese beispielhaft für zwei betrachtete Maßnahmen: „Sicherung der Eintrittspunkte“ und „Externes Audit der Sicherheitsarchitektur“ zur Reduktion des Bedrohungsgrads und der Verwundbarkeit der SaaS-Anwendung. Der Nutzen des Maßnahmenbündels ergibt sich aus der Erhöhung des Sicherheitsniveaus und den Ersparnissen durch frühzeitige Korrektur von Schwachstellen. Das *Sicherheitsniveau*[3] wird in diesem Beispiel anhand der Reduktion von Angriffen und der als schwerwiegend eingestuften Schwachstellen gemessen. Die Kosten der Bedrohungsanalyse und der Maßnahmen sind ebenfalls abgebildet. „Sicherung der Eintrittspunkte“ wirkt sich auf die Indikatoren der *Angriffsfläche* und der *sicheren Implementierung* aus. Die Maßnahmeneffekte auf den *Bedrohungsgrad* können durch Reduktionen von, durch nicht ausreichend gesicherte Eintrittspunkte verursachte, Angriffe analysiert werden. Effekte auf die *Verwundbarkeit* können über die mit den Maßnahmen assoziierten Schwachstellentypen wie Cross-Site-Scripting (XSS) gemessen werden. Die zweite Maßnahme führt zu einer frühzeitigen Erkennung insbesondere konzeptioneller Schwachstellen, wie etwa der Verwendung unsicherer Verschlüsselungsverfahren, und wirkt sich somit auf die Ersparniskomponente aus.

Eine automatisierte Bewertung des Nutzens einzelner Sicherheitsmaßnahmen ist beispielsweise durch die Verwendung von Klassen zur Ursachenkennzeichnung von Angriffen und Schwachstellen möglich. Die Klassen sollten einen Abstraktionsgrad aufweisen, der es erlaubt, Schwachstellen-Ursachen aggregiert darzustellen und einheitlichen Korrekturmaßnahmen gegenüberzustellen. Neben den in Kap. 3 vorgestellten Kennzahlen zur Messung der *Angriffsfläche* sind detailliertere Analysen durch feingranularere Ursachenkategorien möglich, z.B. durch die Differenzierung von Eintrittspunkten in ungesicherte Formularfelder und Authentifizierungsmethoden. In unserem Szenario wird angenommen, dass bei der Behandlung von Angriffen entsprechende voneinander unabhängige Ursachen-Klassen vermerkt werden.

Durch deskriptive Statistiken können Veränderungen der Angriffshäufigkeiten gemessen werden. Durch logistische Regressionen kann der Effekt der Maßnahme auf die Angriffe sowie auf Angriffsursachen gemessen werden. Diese werden durch folgende Modelle dargestellt:

$$Angriff = \beta_1 + \beta_2 * Maßn + \varepsilon_A \quad (3)$$

$$Ursache\_EP = \beta_3 + \beta_4 * Maßn + \varepsilon_{EP} \quad (4)$$

$$Ursache\_KK = \beta_5 + \beta_6 * Maßn + \varepsilon_{KK} \quad (5)$$

Da die abhängigen Variablen binär modelliert werden, sind logistische Regressionen zu verwenden. Beispielsweise erhält *Angriff* den Wert 1, wenn am Tag ein Angriff

[3] Kennzahlen und Indikatoren sind zur besseren Lesbarkeit *kursiv* dargestellt.

stattgefunden hat und ansonsten 0. Somit können die β-Werte in das leicht zu interpretierende Quotenverhältnis (odds ratio - OR) transformiert werden. Die Information, ob ein Angriff in der Periode vor oder nach der Maßnahmeneinführung stattgefunden hat, wird auch mittels binärer Dummy-Variablen abgebildet (β_2, β_4, β_6). Darüber hinaus können durch χ^2-basierte Tests wie den Wald-Test oder den χ^2-Vierfeldertest überprüft werden, ob die Maßnahme zu signifikanten Änderungen geführt hat. Tab. 1 stellt die Ergebnisse der Bewertung der *Angriffsfläche* als Indikator des Bedrohungsgrads dar. Die Zahlen sind beispielhaft gewählt, es geht um die Verdeutlichung des Auswertungsprinzips[4]. Durch logistische Regressionen werden die durch die Maßnahme erzielten Veränderungsraten der Angriffsursachen gemessen (vgl. links in Tab. 1). Insgesamt sind die Angriffe nach Maßnahmendurchführung um 88% gesunken (β_2). Im Anwendungsbeispiel ist die hochsignifikante Angriffswahrscheinlichkeit auf Basis unsicherer Eingabefelder um 92% gesunken (β_4), was als Erfolg der Maßnahme interpretiert werden kann. Die durch unsichere Kommunikationskanäle verursachten Angriffe sind um 47% gesunken (β_6). Offensichtlich hat die Maßnahme auch zur Sicherung unsicheren KKs beigetragen. Die Ergebnisse des χ^2-Unabhängigkeitstests mit 1 Freiheitsgrad in der unteren Zeile zeigen bei Irrtumswahrscheinlichkeiten von weniger als 1%, dass die Reduktion der Angriffe und Angriffsursachen durch die Maßnahme verursacht wurden (s. unterste Zeile). Verteilungsberechnungen zeigen darüber hinaus, dass vor Maßnahmenumsetzung 56% der Angriffsursachen durch unsichere EP erzeugt wurden, danach nur noch 9%. Angriffe durch unsichere KK haben sich um 9% reduziert.

Tab. 1. Ergebnisse der Regressionen und χ2 -Tests

*** p < 0,001,** p < 0,01, *p< 0,05; EP=Eintrittspunkte, KK=Kommunikationskanäle, N= 318 Datensätze, sign.=signifikant, Dstr=Distribut.

Bedrohungsgrad - Angriffsfläche					
Angriffe		Ursache_EP		Ursache_KK	
β_2=-2,11**	OR(β_2)=12	β_4(EP)=-2,5**	OR(β_4)=8%	β_6(KK)=-0,64*	OR(β_6)=53%
Ergebnisse χ^2-Test für χ^2krit.(0,999;1) = 6,635, n=159 paarw. Beobachtungen					
109,1> χ^2krit.→sign.		88,72> χ^2krit. →sign.		13,28> χ^2krit.→ sign.	

Maßn	# Ds	Inc_{Dstr}	EP_{Dstr}	KK_{Dstr}
0	159	74%	56%	23%
1	159	26%	9%	14%
diff	318	48%	47%	9%

Zur Bewertung der *sicheren Implementierung* als Indikator der *Verwundbarkeit* können analog zum *Bedrohungsgrad* einzelne Schwachstellentypen in Abhängigkeit der Maßnahme modelliert werden. Z.B. kann folgendes Modell zur Bewertung des Maßnahmeneinflusses auf die XSS-Schwachstellen herangezogen werden: $Typ_{XSS} = \beta_7 + \beta_8 * Maßn + \varepsilon_{XSS.}$ Darüber hinaus können durch $Schwachstelle_{SCHWER} = \beta_9 + \beta_{10} * Maßn + \varepsilon_{SCHWER}$ die Maßnahmeneffekte auf die unternehmensindividuell schwer eingestuften Schwachstellen[5] bestimmt werden.

[4] Die Verfügbarkeit und Veröffentlichung IT-sicherheitsrelevanter Unternehmensdaten sind bekannte Herausforderungen. Daher wird zunächst nur die Machbarkeit der statistischen Berechnungen anhand eines fiktiven Beispiels demonstriert.

[5] Das sind Schwachstellen, deren Ausnutzung zu hohen finanziellen Auswirkungen führen können.

4.3 Indikatoren zur Nutzenbewertung der Bedrohungsanalyse

QUANTSEC kann auch zur Bewertung übergeordneter Sicherheitsmaßnahmen wie der Bedrohungsanalyse eingesetzt werden. Das Vorgehen dazu wird kurz skizziert. Zunächst sind ökonomische Einflussfaktoren auf den Nutzen der Bedrohungsanalyse zu identifizieren. Dazu zählt der Umfang der Modellierung, da nur das Risiko modellierter Elemente bewertet wird. Durch den Anteil berücksichtigter Informationen an Geschäftsprozessen und Systemkomponenten und den verschiedenen Typen modellierter Informationen, wie z.B. Assets, Bedrohungen, Maßnahmen und Schwachstellen, bestimmen sich Modell-Abdeckungsgrad und -Detailtiefe. Die Bewertungsmethodik ist ein weiterer Einflussfaktor, da nicht angemessen bewertete Bedrohungen zu einem unzureichenden Schutz führen. Somit ermöglicht die Analyse, inwiefern eine Bedrohung in der Bedrohungsanalyse modelliert und richtig bewertet wurde, Rückschlüsse über Effektivität von Bedrohungsmodellierung und Risikobewertung. Dazu ist eine Rückkopplung zwischen einem Angriff, der ausgenutzten Schwachstelle und der dazugehörigen Bedrohung aus der Bedrohungsanalyse notwendig, die über Lokalisierungsdaten der Angriffe und Schwachstellen erfolgen kann. Der Aufwand für solch eine Zuordnung wird in den Interviews erörtert. Neben diesen, der Bedrohungsanalyse direkt zugeordneten Nutzenindikatoren, kann die Bedrohungsanalyse in Anl. an [9] durch die Nutzenbewertung der aus ihren Handlungsempfehlungen resultierenden Sicherheitsmaßnahmen ergänzt werden (s. Beschreibung in Kap. 4.2).

Zusammenfassend kann gesagt werden, dass das Vorgehen zur Anwendung von QUANTSEC die objektive Messung der Effekte von Sicherheitsmaßnahmen im Nachhinein ermöglicht. Der Nutzen kann durch Reflektionen über nützliche Analysen und dazu benötigter Kennzahlen, wie beispielhaft die Klassifizierung von Ursachen im Anwendungsszenario, erhöht werden. Zudem lassen sich die Daten zur Rechtfertigung von zu tätigenden Sicherheitsmaßnahmen und Verbesserungen verwenden. In der Regel werden die gemessenen Daten bereits bei den Entwicklern und Experten vorhandenes, jedoch numerisch nicht belegtes Wissen, bestätigen. Die Datenanalysen können zudem neue Zusammenhänge aufdecken.

In den Beispielen wurden numerische Werte verwendet. Die Zuordnung dieser Daten mit Aufwandsdaten, z.B. Arbeitszeiten für die Behebung verschiedener Schwachstellen-Klassen, die nicht personenbezogen erfolgen muss, ermöglicht weiterführende Analysen, z.B. die Ermittlung der finanziellen Korrekturaufwände einzelner Schwachstellenklassen, auf die in dieser Arbeit nicht weiter eingegangen wird.

5 Erste Modellvalidierung durch Experteninterviews

Die praktische Anwendbarkeit und Angemessenheit des Modells wurde durch erste Interviews mit Experten aus der Praxis überprüft. Zielsetzung war die Überprüfung der Wirkungszusammenhänge und der Korrektheit und Vollständigkeit der Komponenten und Indikatoren sowie der Verfügbarkeit der erforderlichen Kennzahlen in den Unternehmenssystemen. Für nicht oder selten erfasste Kennzahlen wurde der Messaufwand hinterfragt. Dazu wurden jeweils einstündige Interviews mit sechs Experten aus der Softwareentwicklung (E1), der IT-Beratung (E2, E3, E4) und zwei Großun-

ternehmen (E5, E6) geführt. Um eine breite Kompetenzabdeckung zu erhalten, wurden technische IT-Sicherheits- wie auch Sicherheitsmanagement-Experten mit durchschnittlich zehn Jahren Berufserfahrung in der IT-Sicherheit befragt. Aus Platzgründen stellen wir nicht alle Interviewfragen in Tab. 2 dar, sondern beschränken uns auf eine Auswahl von für die Anwendung des Modells elementaren und für unseren Beitrag direkt relevanten oder nicht offensichtlich vorhandenen oder potenziell schwierig erfassbaren Kennzahlen und deren Messaufwände. Beispielsweise werden für Berechnung der Ersparniskomponente **S** Daten zur Schwachstellenentstehungs- und Korrekturphase und die einmalig empirisch erhobenen Korrekturkosten benötigt. Wir präsentieren in Tab. 2 nur die Antworten zur automatisierten Ermittlung der Entstehungsphase und zum Vorhandensein von Korrekturkosten, da diese nicht offensichtlich gegeben sind. Offene Antworten zu den vorgestellten Fragen sowie Antworten zur Bewertung der Erhebungsaufwände der Nutzenindikatoren der Bedrohungsanalyse werden im Text beschrieben. Links dargestellt in Tab. 2 sind die Modellkomponenten (MK), in denen die befragten Kennzahlen Anwendung finden: Ersparniskomponente **L,** Kostenkomponente **C** und **S**. Die Spalten rechts geben Auskunft über den Mittelwert (MW) und die Anzahl der erhaltenen Antworten (N). Abkürzungen und Skalen sind der Legende oben zu entnehmen.

Tab. 2. Interview-Ergebnisse

Legende: SWH=SW Hersteller, MK= Modellkomponente, U= Unternehmen, GU= große Unternhmen, #= Angriffshäufigkei, MW = Mittelwert, i.W: im Wesentlichen; Skalen: Y= 1 (sehr gut) - 5 (sehr schlecht); Z = 1 (stimme voll zu) - 5 (stimme gar nicht zu)

MK			Frage	Skala	SWH	IT-Beratungen			GU		MW	N
					E1	E2	E3	E4	E5	E6		
Modell-validierung		L	"Die **Verwundbarkeit** einer SW hängt i.W. ab von 1. der **sicheren Implementierung** sowie 2. der **Erkennung** von Schwachstellen und 3. der **Korrektur** von Schwachstellen"	Z	2	1	1	1	1	2,5	**1,4**	**6**
		L	Inwieweit können auf Basis der drei Kategorien 1, **Angriffsfläche,** 2. **Verbreitungsgrad** und 3. **Anzahl an Angriffs und Angriffsversuchen** Rückschlüsse über den **Bedrohungsgrad** einer SW gezogen werden?	Y	3	2	2	2	1	2,5	**2,1**	**6**
		L	**Wichtigste** der drei genannten **Kategorien** zur Bestimmung des Bedrohungsgrads: A: Angriffsfläche, B: Verbreitungsgrad und C: Anzahl an Angriffe und Angriffsversuchen		N/A	C	C	C	C	A		**5**
Datenverfügbarkeit	#	L	**Anzahl der Sicherheitsvorfälle** (✓→ Daten liegen vor, (✓) → Daten liegen in GU vor)		✓	✓	(✓)	✓	✓	✓		**6**
	Verwund-barkeit	L, S	"Die **Entstehungsphase** von Schwachstellen lässt sich eindeutig zuordnen"	Z	1	N/A	2	2	1	3	**1,8**	**5**
		L	**Auswertung von Angriffsversuchen (z. B. mit Security-Information-and-Event-Management-Systemen)** (✓ Daten liegen in GU vor)		✓	✓	✓	✓	✓	✓		**6**
	Kosten von Maßnahmen	**Korrektur von Schwachstellen**										
		S, C	**Benötigte Arbeitszeit** (✓ → Daten liegen vor, (✓) →Daten liegen in GU vor, (ISO) "Daten liegen bei ISO-27001-zertifizierten U vor , (✗) →Selten erfasst; nur für in Rechnung zu stellende Leistungen)		✓	ISO	(✓)	N/A	✓	(✗)		
			Messbarkeit der Arbeitszeit	Y	N/A	2	2	2	1	N/A	**1,8**	**4**
		Implementierung von Maßnahmen										
		S, C	**Benötigte Arbeitszeit** (✓ " Daten liegen vor, (✓) "liegen nur qualitativ vor , (ISO) "Daten liegen bei ISO-27001-zertifizierten U vor , (✗) "Daten liegen nicht vor)		✓	ISO	✗	✗	N/A	(✓)		
			Messbarkeit der Arbeitszeit	Y	N/A	2	4	2	N/A	N/A	**2,7**	**3**

Die beiden Fragen zur Modellvalidierung, d.h. der Indikatoren zur Abbildung der Verwundbarkeit und des Bedrohungsgrads, wurden von allen Befragten (N=6) mit hohen Werten, MW: 1,42 und MW: 2,1 auf 5er-Likert-Skalen[6], bestätigt. Insbesondere die Abbildung des Bedrohungsgrads von SW-Anwendungen auf Indikatoren ist nicht trivial, so dass 2,1 einem sehr guten Zustimmungswert darstellt. Als ergänzende Kriterien wurden die *Exponiertheit* (E5) und die *Sensitivität der Daten* (E3) genannt.

[6] Der Wert 1: entspricht „sehr gut" bzw. „stimme voll zu", der Wert 5 bedeutet „sehr schlecht" bzw. „stimme gar nicht zu".

Die Exponiertheit beschreibt die Zugriffsmöglichkeiten und den Zugriffsaufwand für Angreifer, die Sensitivität die Schutzwürdigkeit enthaltener Daten. Wenn keine detaillierten Daten verfügbar sind, kann die Exponiertheit z.B. mit einer Dummy-Variable operationalisiert werden, die 1 ist, wenn eine Anwendung über das Internet verfügbar ist, 0 andernfalls. Es herrschte Einigkeit, dass besonders in großen Unternehmen Daten zur Häufigkeit von Sicherheitsvorfällen vorliegen (N=6). Deren Auswertbarkeit über die Zeit zur Operationalisierung der Angriffsversuche, wurde bestätigt, ebenso die Verfügbarkeit von Lokalisationsdaten ausgenutzter Schwachstellen auf Komponentenebene (N=4), insbesondere für große Unternehmen (N=5). Zur Messung der Indikatoren der Verwundbarkeit wird die durchschnittliche Schwachstellenerkennungs- und Korrekturzeit benötigt. Der dazu notwendige Entstehungszeitpunkt scheint keine gängig vorhandene Information zu sein, doch vier Experten meinten, dass die Rückverfolgung möglich sei, z.B. auf Grundlage von Codeverwaltungs-SW (N=4: E1, E3, E4, E6). Die Zuordnungsmöglichkeit der Entstehungsphase, z.B. Design, Coding oder Testing, zum Entstehungszeitpunkt wurde mehrheitlich zugestimmt (MW: 1,8; N=5). Diese Kennzahlen werden für die Berechnungen der Ersparniskomponente S und der Kostenfaktoren für die Schwachstellenkorrekturen benötigt. Für die Ersparnis und die Kostenkomponente werden Daten zu Arbeitszeiten für Schwachstellenkorrekturen und Maßnahmenimplementierungen benötigt. Die Korrekturzeiten scheinen in großen und insbesondere bei ISO-27001-zertifizierten Unternehmen vorzuliegen (N=3). Die Messbarkeit dieser Daten wird mit gut bewertet, wobei jedoch auf Datenschutzaspekte zu achten wäre. Benötigte Arbeitszeiten für Maßnahmenimplementierungen liegen eher nicht vor. Nur E1 bestätigte die Verfügbarkeit, E2 bestätigte sie für die meisten zertifizierte Unternehmen. Die generelle Messbarkeit wurde als mittelmäßig bewertet. Die Machbarkeit und der Aufwand für die Rückverfolgung von Angriffen auf die Bedrohungsanalyse wurde durch zwei Fragen adressiert: Der Aufwand zur Identifizierung, ob und wie ein Angriff modelliert wurde, um die Angemessenheit des Modellierungsumfangs bewerten zu können, schätzten drei Experten (E3, E5, E6) als hoch ein, wiesen jedoch teils auf die starke Abhängigkeit des Aufwands von der Geschäftslogik hin (E3). E1 meinte, dass Untersuchungen zur automatisierten Prüfung bereits implementiert seien. Auf die Frage, inwiefern ein CVSS-Mapping des Angriffs und zugehörigem Angriffsszenario sinnvoll sei, um zu prüfen, wie korrekt das Angriffspotenzial bewertet wurde, wurde von drei Experten (E1, E5, E6) als sinnvoll erachtet. Im Allgemeinen scheint die Abbildungsmöglichkeit sehr von der unternehmensindividuellen Ausgestaltung der Bedrohungsanalyse abzuhängen.

Zusammenfassend lässt sich sagen, dass Bedarf und Nutzen des Modells von allen Befragten bekräftigt und die grundlegenden Wirkungszusammenhänge des Modells zu dessen Validierung bestätigt wurden. Insbesondere bei großen Unternehmen scheinen die elementaren Daten zur Modellanwendung vorzuliegen oder es besteht großes Potenzial zur Erhebung weiterer Kennzahlen mit relativ geringem Aufwand.

6 Fazit, kritische Betrachtung und weitere Schritte

6.1 Fazit

Es wurde ein Modell zur Analyse von Sicherheitsattributen und zur Bewertung des ökonomischen Nutzens von IT-Sicherheitsmaßnahmen vorgestellt, das auf objektiven Kennzahlen zur automatisierten Messung basiert. Das Modell QUANTSEC beruht auf der Zusammenführung ökonomischer und technischer Modelle unterschiedlichen Abstraktionsgrads und der Erarbeitung von Wirkungsbeziehungen zwischen den unterschiedlichen Modellkategorien. Durch statistische Auswertungen der Unternehmensdaten lassen sich sowohl generelle Wirkungsbeziehungen der Kennzahlen zueinander objektiv ermitteln und belegen wie auch die Effektstärke und Nutzen der durchgeführten Maßnahmen auf die einzelnen, im Modell definierten, Kennzahlen. Dies ermöglicht differenzierte Aussagen über den Nutzen durchgeführter Maßnahmen in Bezug auf das IT-Sicherheitsniveau sowie über die Verwundbarkeit und den Bedrohungsgrad von Systemen oder Anwendungen. Hierdurch können auch neuralgische Punkte, für die starke Effekte z.B. auf die Angriffshäufigkeit gemessen wurden, identifiziert und somit konkrete Verbesserungspotenziale für die Durchführung künftiger Sicherheitsmaßnahmen abgeleitet werden. Die Verfügbarkeit der hauptsächlichen relevanten Daten zur Modelanwendung konnte für große Unternehmen bestätigt werden. Die Datenverfügbarkeit bei kleinen und mittleren Unternehmen hingegen scheint nicht gewährleistet, so dass QUANTSEC eher für große Unternehmen anwendbar erscheint.

Durch die Einbeziehung ökonomischer Kennzahlen, wie z.B. den spezifischen Kosten zur Angriffsbehandlung, können die statistischen Analysen mit finanziellen Informationen angereichert werden. Für die letztendliche Bewertung des monetären Nutzens von Maßnahmen wurde neben der Schadens- und der Kostenkomponente die Ersparniskomponente integriert, mit der zusätzlich generierte Kostenersparnisse durch frühzeitige Schwachstellenkorrektur auf Basis unternehmensspezifischer Kostensätze monetär berechnet werden können.

6.2 Kritische Betrachtung und weitere Schritte

Durch die Experteninterviews wurde eine erste vorläufige Evaluation des Modells vorgenommen, wodurch dessen Wirkungsweise, dessen Nutzen und Einsetzbarkeit in der Praxis prinzipiell validiert wurde. Die Anzahl der befragten Experten ist nicht groß genug zur Verallgemeinerung der Aussagen. Daher planen wir eine großflächige empirische Studie des Modells auf Grundlage eines Fragebogens und eine prototypische Umsetzung für die Datenauswertung und -analyse.

Das Vorgehen zur statistischen Datenauswertung wurde nur grundlegend beschrieben. Weiterführende Methoden sind notwendig, um z.B. den aggregierten Einfluss mehrerer Indikatoren auf eine übergeordnete Bezugsgröße wie der Verwundbarkeit quantifizieren zu können. Eine Lösung hierzu könnte Maarten Buis Ansatz zur statis-

tischen Kombination mehrerer Variablen auf Basis von Sheaf coeffcients zur Berechnung von latenten Variablen in [14] sein.

Diese Arbeit wurde durch das Bundesministerium für Bildung und Forschung im Rahmen von EC SPRIDE gefördert.

Literatur

1. Neubauer, Thomas, Hartl, Christian: On the Singularity of Valuating IT Security Investments. In: Proceedings of the 2009 Eigth IEEE/ACIS International Conference on Computer and Information Science. Washington, DC, USA (2009)
2. Böhme, R., Nowey, T.: Economic security metrics. In: Irene, E., Felix, F., Ralf, R. (Eds.), Dependability Metrics, 4909, S.176–187 (2008)
3. Soo Hoo, K.J.: How Much is Enough: A Risk Management Approach to Computer Security. Dissertation, Stanford University: Stanford, CA, USA (2000)
4. Jones, J.: Risk Taxonomy. In: The Open Group – Technischer Bericht, http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf (2009)
5. Sonnenreich, W., Albanese, J., Stout, B., Return On Security Investment (ROSI): A Practical Quantitative Model. In: Journal of Research and Practice in Information Technology 38.1, S.45-56 (2006)
6. Fox, D.: Betriebswirtschaftliche Bewertung von Security Investments in der Praxis. In: Datenschutz und Datensicherheit 35, S.50–55 (2011)
7. Arora, A., Hall, D, Pinto, A., Ramsey, D., Telang, R.: An ounce of prevention vs. a pound of cure: How can we measure the value of IT security solutions? Lawrence Berkeley National Laboratory, University of California – Technischer Bericht (2004)
8. Chen, Y., Boehm, B., Measuring Security Investment Benefit for Off the Shelf Software Systems - A Stakeholder Value Driven Approach. In: Workshop on the Economics of Information Security (2007)
9. Lockstep Consulting: Government Chief Information Office: A Guide for Government Agencies Calculating Return on Security Investment (2004)
10. Rudolph, M., Schwarz, R.: Security Indicators - A State of the Art Survey. Fraunhofer IESE – Technischer Bericht (2012)
11. Brecht, M., Nowey, T.: A Closer Look at Information Security Costs. In: 11th Annual Workshop on the Economics of Information Security, Berlin (2012)
12. National Institute of Standards and Technology: The economic impacts of inadequate infrastructure for software testing (2002)
13. Manadhata, Pratyusa K., Wing, Jeannette M.: An Attack Surface Metric. In: IEEE Transactions on Software Engineering 37.3, S.371-386 (2011)
14. Buis, M.: Combining information from multiple variables using models for causal indicators. Universität Tübingen – Technischer Bericht (2014)